Vol. 4 No. 2 May 2011

Pro Te: *Solutio*

SOLUTIONS FOR YOU

Proof Of Knowledge Not Required

The Federal Government's Power To Prosecute Healthcare Executives

State Security Breach Notification Laws

Enhancing The Protection Of Personal Information

Dear Client:

Many in the industry have watched with concern the increasing numbers of criminal prosecutions of healthcare executives for corporate fraud. *Proof of Knowledge (or Participation or Intent) Not Required* explores the Federal Government's use of *United States v. Park* and the "Responsible Corporate Officer" doctrine to prosecute and exclude corporate healthcare executives. Given this environment and its serious implications for healthcare executives as well as the industry, considerations for procedures and compliance issues are suggested. Also provided is timely advice on how to minimize the risk of potential liability.

Another area of increasing risk is security breaches and how well or poorly a company responds when breaches happen. Forty-six states have statutes that direct what must be done when a breach occurs, and a company can face substantial fines for not complying with these statutes. *State Security Breach Notification Laws* gives in-depth analysis of how states have come to deal with security breaches as well as citations to all of these statutes.

Our final article is a preview of things to come. The HIPAA regulations that we have been following for years will be changing soon. As we await the final regulations, *Coming Soon: HIPAA Gets a Facelift* will give you a glimpse into what to expect.

Butler Snow helps clients manage the risk of human and technological failings by thinking ahead and by staying abreast of regulatory and other industry changes. We hope this issue of *Pro Te: Solutio* provides helpful insight into the challenges facing the industry.

Christy D. Jones
Co-Chair — Litigation

Charles F. Johnson
Co-Chair —
Business and Corporate Healthcare

Pro Te: *Solutio*

Vol. 4 No. 2 May 2011

Sharing Solutions

It's human nature to share problems. But how often is someone willing to share solutions? Butler Snow wants to do just that — provide scenarios and the solutions that turned a client's anxiety into relief and even triumph. That's why we created this magazine, *Pro Te: Solutio*, which explores how real-life legal problems have been successfully solved.

That's also why we at Butler Snow redesigned and expanded our unique health-oriented industry group, now comprised of two major sections that handle business and litigation. The Pharmaceutical, Medical Device, and Healthcare Industry Group has more than 50 multi-disciplinary attorneys who provide creative solutions for the complex issues of the healthcare industry. This group includes product liability and commercial litigators; corporate, commercial, and transaction attorneys; labor and employment attorneys; intellectual property attorneys; and those experienced in government investigations.

Pro Te: Solutio is a quarterly magazine available only to the clients of Butler Snow. If you have questions or comments about its articles, you're invited to contact Christy Jones and Charles Johnson, as well as any of the attorneys listed on the inside back cover of this publication.

TABLE *of* CONTENTS

PROOF OF KNOWLEDGE (OR PARTICIPATION OR INTENT) NOT REQUIRED

The Federal Government's Use of United States v. Park *and the "Responsible Corporate Officer" Doctrine to Prosecute and Exclude Corporate Healthcare Executive*

I. Introduction

Consider the following words of Chief Justice Warren Burger from the 1975 decision, *United States v. Park,* 421 U.S. 658:

> *The requirements of foresight and vigilance imposed on responsible corporate agents are beyond question demanding, and perhaps onerous, but they are no more stringent than the public has a right to expect of those who voluntarily assume positions of authority in business enterprises whose services and products affect the health and well-being of the public that supports them.*

Nearly forty years later, this commentary resounds in the healthcare industry. Federal agencies tasked with policing fraud and abuse in the healthcare industry increasingly are relying upon the *Park* "responsible corporate officer" doctrine to investigate and impose severe criminal and civil penalties on healthcare industry executives. The U.S. Department of Health and Human Services Office of Inspector General (OIG) and the Food and Drug Administration (FDA) are wielding two swords in their efforts to address corporate fraud in healthcare: criminal prosecution and exclusion from federally funded healthcare programs.

II. An Environment Ripe with Criminal Prosecutions and Civil Sanctions

A. Criminal Prosecutions

On the criminal front, the federal government has articulated its intent to pursue more prosecutions against healthcare executives for charges (including misdemeanors) under the federal Food, Drug, and Cosmetic Act (FDCA). Significantly, these "*Park* Doctrine" prosecutions *do not* require proof that the corporate officers had any actual knowledge of, or participation in, specific offenses. To this point, the FDA recently added to its Regulatory Procedures Manual (RPM) a new provision directly targeted at healthcare industry executives.[1] RPM Section 6-5-3, "Special Procedures and Considerations for *Park* Doctrine Prosecutions," provides:

> The *Park* Doctrine, as established by Supreme Court case law, provides that a *responsible corporate official can be held liable for a first time misdemeanor (and possible subsequent felony) under the Federal Food, Drug, and Cosmetic Act ("the Act") without proof that the corporate official acted with intent or even negligence, and even if such corporate official did not have any actual knowledge of, or participation in, the specific offense.* A *Park* Doctrine prosecution, for the purposes of this section, refers to a recommended prosecution of a responsible corporate official for a misdemeanor violation of the Act.[2]

Among the factors FDA considers are the individual's position in the company, his relationship to the violation, and whether he had the authority to correct or prevent the violation. Other relevant factors include (1) whether the violation involves actual or potential harm to the public, (2) whether the violation is obvious, (3) whether the violation reflects a pattern of illegal behavior and/or failure to heed prior warnings, (4) whether the violation is widespread, (5) whether the violation is serious, (6) the quality of the legal and factual support for the

proposed prosecution, and (7) whether the proposed prosecution is a prudent use of agency resources.

Section 6-5-3 further reiterates that "[k]nowledge of and actual participation in the violation are not a prerequisite to a misdemeanor prosecution but are factors that may be relevant when deciding whether to recommend charging a misdemeanor violation." Thus, under the *Park* Doctrine and FDA policy, a corporate healthcare executive may be charged with a misdemeanor offense for healthcare fraud — even without proof of participation in the specific offense, intent, actual knowledge, or even negligence.

B. Exclusion from Federal Healthcare Programs

A "*Park* Doctrine" conviction can lead not only to criminal penalties but also to additional sanctions in the form of an "exclusion." RPM Section 6-5-3 clearly states that "[i]n some cases, a misdemeanor conviction of an individual may serve as the basis for debarment by FDA." A "debarment" or "exclusion" prevents an individual or entity from participating in federally-funded healthcare programs.[3] The period of time for the exclusion varies based on the specific offense.[4]

The effects of an exclusion are far-reaching, especially given the significant revenue stream that federal health programs provide to the healthcare industry. Exclusion[5] can mean:

- No payment will be made by any federal healthcare program for any items or services furnished, ordered, or prescribed by an excluded individual or entity (there is a limited exception for certain emergency items or services).
- No program payment will be made for anything that an excluded person furnishes, orders, or prescribes; this prohibition applies to the excluded person, anyone who employs or contracts with the excluded person, any hospital or other provider where the excluded person provides services, and anyone else.

Exclusions fall under the purview of the OIG, an independent nonpartisan agency within the United States Department of Health & Human Services (HHS).[6] But make no mistake, OIG is a law enforcement agency. Among other responsibilities, OIG investigates suspected fraud, refers cases to the United States Department of Justice (DOJ) for criminal and civil actions, and imposes monetary penalties or exclusions from participation in federal healthcare programs. In its healthcare fraud enforcement role, OIG works closely with DOJ, law enforcement partners, the Centers for Medicare and Medicaid Services, and FDA.

OIG's investigations in the healthcare industry address a wide range of fraudulent healthcare schemes (e.g., phony clinics, fraudulent billing) on a number of levels — from small operators to major organized crime rings. Of note here, however, are the OIG's recent public pronouncements of its intention to target major corporations, such as pharmaceutical and medical device manufacturers, whom the OIG contends "have also committed fraud, sometimes on a grand scale."[7] In recent Congressional testimony, OIG asserted that "[s]ome hospital systems, pharmaceutical manufacturers, and other providers play such a critical role in the care delivery system that they may believe that they are 'too big to fire' and thus OIG would never exclude them […]."[8] Stating its concern that major corporations "may consider civil penalties and criminal fines a cost of doing business," OIG seeks to "alter the cost-benefit calculus of the corporate executives who run these companies" by "excluding" individuals who are responsible for the fraud, either directly or because of their positions in the company that engaged in fraud.[9]

The authority to exclude individuals and entities from participation in federal healthcare programs is found in Section 1128 of the Social Security Act.[10] This provision authorizes the Secretary of HHS to exclude individuals or entities — on either a mandatory or permissive basis — under the following categories of conduct[11]:

Section 1128: Mandatory and Permissive Exclusions

Mandatory Exclusions (Section 1128(a))	(1) Conviction of program-related crimes (2) Conviction relating to patient abuse (3) Felony conviction relating to healthcare fraud (4) Felony conviction relating to controlled substance
Permissive Exclusions (Section 1128(b))	(1) Conviction relating to fraud (2) Conviction relating to obstruction of an investigation or audit (3) Misdemeanor conviction relating to controlled substance (4) License revocation or suspension (5) Exclusion or suspension under federal or state healthcare program (6) Claims for excessive charges or unnecessary services and failure of certain organizations to furnish medically necessary services (7) Fraud, kickbacks, and other prohibited activities (8) Entities controlled by a sanctioned individual (9) Failure to disclose required information (10) Failure to supply requested information on subcontractors and suppliers (11) Failure to supply payment information (12) Failure to grant immediate access (13) Failure to take corrective action (14) Default on health education loan or scholarship obligations (15) Individuals controlling a sanctioned entity (16) Making false statements or misrepresentation of material facts

Consistent with OIG's intention to target major corporations and executives for healthcare fraud-related crimes, new emphasis has been placed on Section 1128(b)(15) — Individuals Controlling a Sanctioned Entity. In October 2010, OIG released its "Guidance for Implementing Permissive

Exclusion Authority Under Section 1128(b)(15) of the Social Security Act."[12]

Section 1128(b)(15)(A) provides for permissive exclusion of two categories of individuals: those with an *ownership/control interest* in a sanctioned entity[13] and *corporate officers or managing employees*[14] "based solely on their position within the entity."[15] For corporate officers/managing employees, OIG will consider the basis for the criminal conviction and/or exclusion of the entity (i.e., the company) as well as any other conduct that formed the basis for criminal, civil, or administrative investigations, cases, charges, or resolutions.[16] OIG will also consider matters that involve entities that are or were related to the convicted or excluded entity.[17] Moreover, the Guidance spells out relevant factors related to "misconduct."[18] Given the importance of these factors, they are provided, in full, below:

Circumstances of the Misconduct and Seriousness of the Offense

1. What were the nature and scope of the misconduct for which the entity was sanctioned? What were the nature and scope of any other relevant misconduct? At what level of the entity did the misconduct occur (e.g., violation by one field employee of company policy versus headquarters' involvement and/or direction)?

2. What was the criminal sanction imposed against the entity (or related entities) or any individuals? What was the amount of any criminal fine, forfeiture, or penalty imposed? What was the amount of any civil or administrative payment regarding related or similar issues? What was the length of any period of exclusion imposed?

3. Was there evidence that the misconduct resulted in (1) actual or potential harm to beneficiaries or other individuals or (2) financial harm to any Federal healthcare program or any other entity? If financial loss to the programs or other persons occurred, what was the extent?

4. Was the misconduct an isolated incident or part of a pattern of wrongdoing over a significant period of time? Has the entity previously had similar problems with OIG, the Centers for Medicare & Medicaid Services or its contractors, or any other Federal or State regulatory agency? What was the nature of these problems?

Individual's Role in Sanctioned Entity

1. What is the individual's current position? What positions has the individual held with the entity throughout his or her tenure, particularly at the time of the underlying misconduct? What degree of managerial control or authority is involved in the individual's position?
2. What was the relation of the individual's position to the underlying misconduct? Did the misconduct occur within the individual's chain of command?

Individual's Actions in Response to the Misconduct

1. Did the individual take steps to stop the underlying misconduct or mitigate the ill effects of the misconduct (e.g., appropriate disciplinary action against the individuals responsible for the activity that constitutes cause for the sanction or other corrective action)? Did these actions take place before or after the individual had reason to know of an investigation? If the individual can demonstrate either that preventing the misconduct was impossible or that the individual exercised extraordinary care but still could not prevent the conduct, OIG may consider this as a factor weighing against exclusion.

2. Did the individual disclose the misconduct to the appropriate Federal or State authorities? Did the individual cooperate with investigators and prosecutors and respond in a timely manner to lawful requests for documents and evidence regarding the involvement of other individuals in a particular scheme?

Information About the Entity

1. Has the sanctioned entity or a related entity previously been convicted of a crime or found liable, civilly or administratively, or resolved a civil or administrative case with the Federal or State Government or a government entity? If so, what was the prior conduct that formed the basis for these actions?

2. What is the size of the entity? (e.g., how many employees does the entity have, what are the revenues, how many product lines/divisions are there within the entity)? What is the corporate structure of the entity? (e.g., how many subsidiaries — operating and nonoperating — are there, what are the sizes of the subsidiaries, and what are the reporting relationships between the subsidiaries)?

III. Case in Point

A. *Friedman v. Sebelius*: Use of "Agreed Statement of Facts" in Criminal Plea Agreement Subjects Former Executives to Exclusion

A recent and highly publicized case from the United States District Court, District of Columbia, illustrates the close connection between criminal liability and exclusion under the FDCA and Section 1128. In *Friedman v. Sebelius*, 755 F.Supp.2d 98 (D. D.C. 2010), three corporate executives with Purdue Frederick Company — Michael Friedman (former President/CEO), Paul Goldenheim (former Executive VP of Medical and Scientific Affairs/Worldwide Research and Development), and Howard Udell (former Executive VP/Chief Legal Officer) — were investigated, charged, and convicted of misdemeanor offenses and ultimately excluded from participation in all federal healthcare programs for twelve years.[19]

In 2001, the United States Attorney's Office for the Southern District of Virginia began to investigate the marketing and sale of OxyContin, a prescription pain medication manufactured and distributed by Purdue.[20] The investigation revealed that Purdue supervisors and employees marketed and promoted OxyContin as "less addictive, less subject to abuse and diversion, and less likely to cause tolerance and withdrawal than other pain medications."[21] In 2007, federal criminal charges were filed against Purdue for allegedly misbranding a drug with intent to defraud or mislead, a felony under the FDA.[22] The three senior corporate executives were charged as "responsible

corporate officers," a misdemeanor.[23]

Purdue and the three executives entered guilty pleas.[24] Purdue agreed to pay $600 million in monetary penalties.[25] The three corporate executives agreed to disgorge $34.5 million and were sentenced to three years' probation, 400 hours of community service, and a $5,000 fine.[26] Importantly, as part of their plea agreements, the three executives agreed that the Court could accept an "Agreed Statement of Facts" that was prepared by the parties.[27]

The facts contained in the Agreed Statement proved to be the lynchpin for the subsequent exclusions of the three executives. After the criminal proceeding was concluded, the Inspector General notified the three executives that, as a result of their criminal convictions, the agency was considering their exclusion pursuant to Section 1128.[28] Four months later, the Secretary of HHS officially excluded the executives. After several administrative hearings and appeals, the executives faced a twelve-year exclusion from participation in all federally funded healthcare programs.[29]

The three executives filed a request for judicial review to challenge the exclusion.[30] The district court first rejected the argument that Section 1128's permissive exclusion provision does not authorize the Secretary of HHS to exclude individuals convicted of misdemeanor misbranding under the *Park* Doctrine (responsible corporate officer) because such convictions do not require any evidence of personal wrongdoing.[31] The court applied a broad meaning to the phrase "misdemeanor *relating to*" fraud and found that the offenses that triggered exclusion were "related to" fraud or financial misconduct.[32] The court further reasoned that the Secretary's decision should be affirmed as reasonable, particularly in light of the fact that the Agreed Statement of Facts (from the criminal plea agreement) specifically acknowledged that the executives were corporate officers with responsibility and authority to prevent or correct the misconduct related to the misbranding of OxyContin.[33]

Friedman is illustrative on a number of levels. First, it showcases how a criminal misdemeanor that carried a comparatively light individual punishment can serve as the basis for exclusion from all federal healthcare programs. Second, it highlights the intensity with which the OIG and FDA will work together (and with other law enforcement) to target high-level executives in the healthcare industry. In recent Congressional testimony, Inspector General Levinson noted that, in addition to excluding the Purdue Frederick executives, the OIG recently excluded the former owner/former executive of Ethex Corporation for twenty years for failing to inform the FDA about manufacturing problems that led to the production of oversized prescription drug tablets.[34]

The U.S. Department of Health and Human Services Office of Inspector General (OIG) and the Food and Drug Administration (FDA) are wielding two swords in their efforts to address corporate fraud in healthcare: criminal prosecution and exclusion from federally funded healthcare programs.

If these stories were not enough, a recent front-page *Wall Street Journal* article undoubtedly sent additional shockwaves through the healthcare industry.[35] The article reports that HHS has notified the CEO of Forest Laboratories, Howard Solomon, that it intends to exclude him under Section 1128. The Forest Laboratories situation differs from the *Friedman*/Purdue Frederick case in an important aspect. In *Friedman*, both the corporation *and* the executives were convicted of federal crimes, and exclusions followed. In the Forest Laboratories case, *only the corporation* was charged with a federal crime, for which it entered into a plea agreement in March 2011. Three weeks later, Solomon was notified of HHS's intent to seek exclusion, notwithstanding the fact that he was not charged with any federal criminal act.

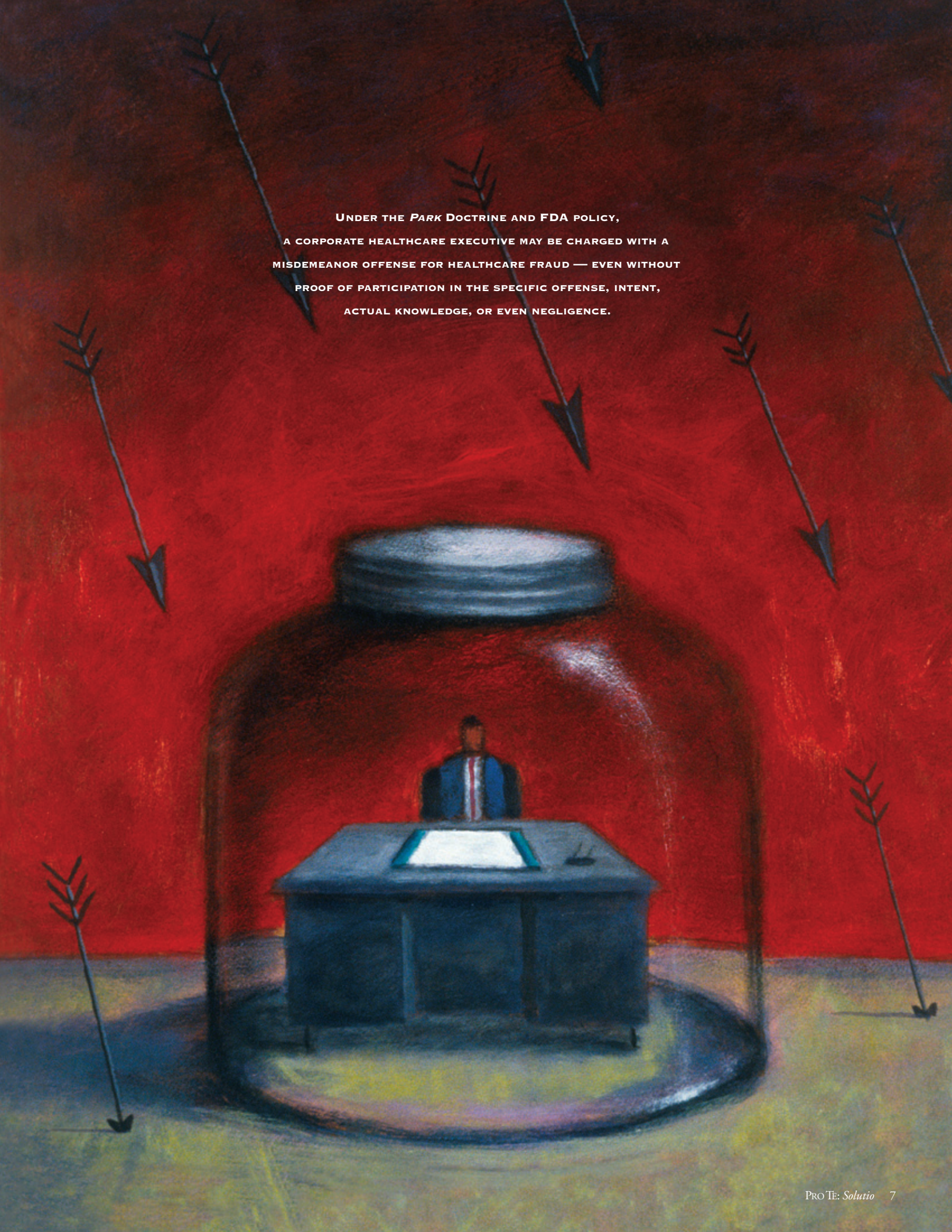
IV. What's Next

A. HHS/DOJ Annual Report: Introducing the Pharmaceutical Fraud Pilot Program (PFPP)

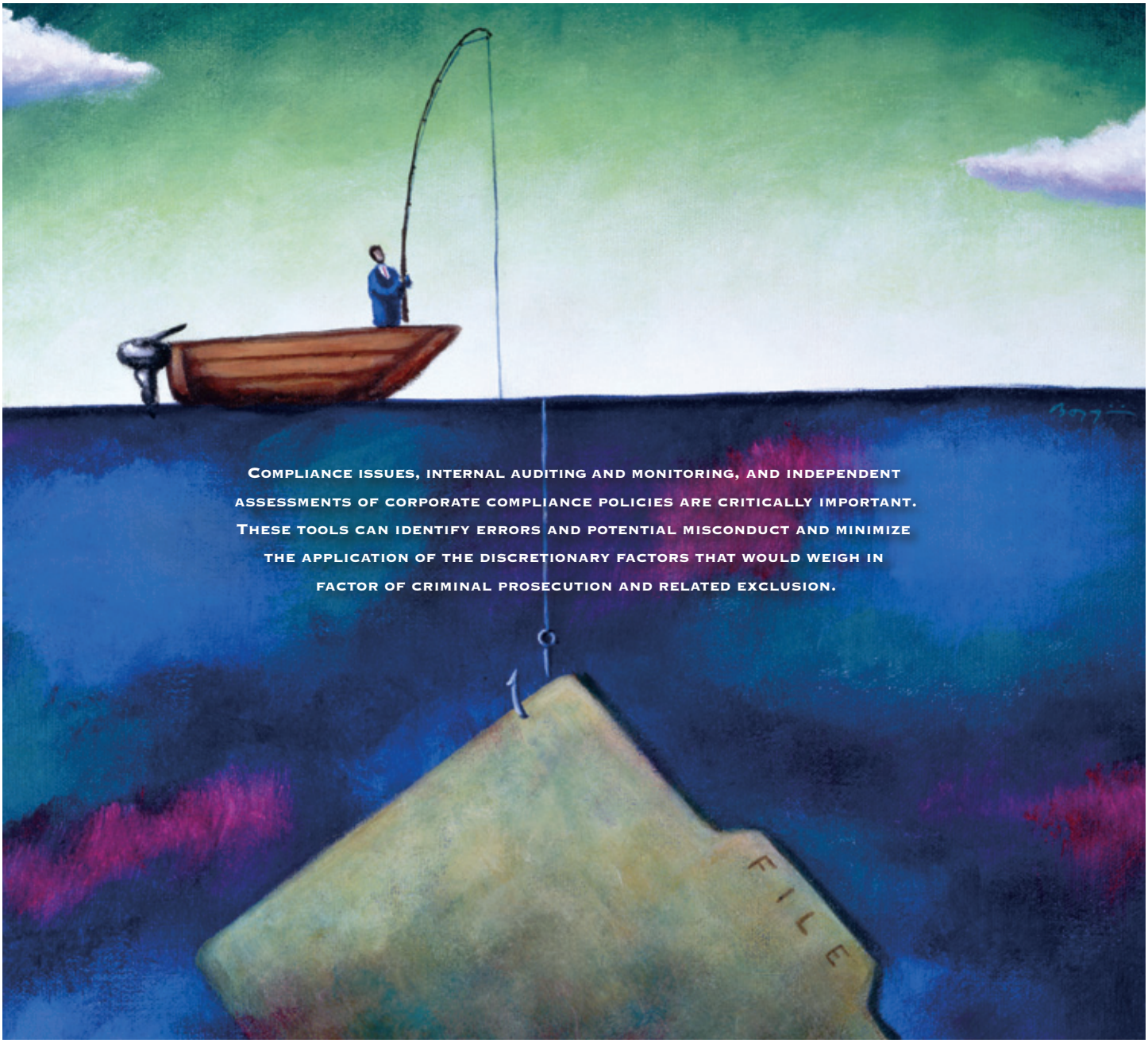
In its FY 2010 Annual Report, the HHS and DOJ Health Care Fraud and Abuse Control Program identified that in FY 2010, the OIG excluded 3,340 individuals and entities.[36] Nearly 40% of these exclusions involved crimes related to Medicare, Medicaid, or other federal healthcare programs.[37] Given the OIG's public announcements and written policies related to enhanced use of exclusions as a "valuable enforcement tool," as well as the FDA's efforts to prosecute corporate executives pursuant to the *Park* Doctrine, these numbers should be expected to increase.

The Annual Report also discussed a $1.7 million allocation in FY 2010 to FDA by HHS for the FDA Pharmaceutical Fraud Pilot Program (PFPP). According to the report, this program has enhanced the healthcare fraud-related activities of FDA's Office of Criminal Investigations which, together with the Office of the General Counsel Food and Drug Division, investigates criminal violations of the FDA and other federal statutes.[38] More specifically, PFPP "is designed to detect, prosecute, and prevent pharmaceutical, biologic, and medical device fraud. The PFPP focuses on fraudulent marketing schemes, application fraud, clinical trial fraud, and flagrant manufacturing-related violations."[39] Likely as a nod to the *Friedman*/Purdue Frederick case, PFPP anticipates investigation of "marketing schemes that knowingly overstate the effectiveness or minimize the risk of a medical product."[40] Moreover, the PFPP comes amidst record healthcare fraud recoveries from pharmaceutical companies in FY 2010, including a single settlement by Pfizer for $2.3 billion.

Review of the Annual Report reveals that the PFPP is in ramp-up mode. FDA



Under the *Park* Doctrine and FDA policy, a corporate healthcare executive may be charged with a misdemeanor offense for healthcare fraud — even without proof of participation in the specific offense, intent, actual knowledge, or even negligence.



Compliance issues, internal auditing and monitoring, and independent assessments of corporate compliance policies are critically important. These tools can identify errors and potential misconduct and minimize the application of the discretionary factors that would weigh in factor of criminal prosecution and related exclusion.

received its approval for the program in FY 2010 and was in the hiring process for personnel. Notwithstanding its new status, FDA noted that through the PFPP it had opened — in a relatively short time — the following criminal investigations: two off-label promotion matters involving different manufacturers of brand name prescription drugs; claims against a third pharmaceutical manufacturer for various promotional issues including overstatement of efficacy, omission of material facts, and promotion of unapproved uses; two matters involving Good Manufacturing Practice issues, one of which also involves potential application and promotional fraud; a clinical trial fraud matter where study documents are alleged to have been falsified by a study coordinator; falsification by a Contract Research Organization company of study documents related to research studies conducted for pharmaceutical manufacturers; and falsification by a Contract Testing Laboratory company of data used to support multiple drug applications.[41]

V. Suggestions

Given this environment for healthcare executives, there is no more important time to evaluate compliance policies and procedures that address industry best practices and minimize the risk of misconduct and the potential for criminal and/or civil liability. As set forth in *Corporate Responsibility and Corporate Compliance: A Resource for Health Care Boards of Directors*,[42] companies should consider compliance questions such as:

• Code of Conduct: How has the Code of Conduct or its equivalent been incorporated into corporate policies across the organization? How do we know that the Code is understood and accepted across the organization? Has management taken

affirmative steps to publicize the importance of the Code to all of its employees?

• Policies and Procedures: Has the organization implemented policies and procedures that address compliance risk areas and established internal controls to counter those vulnerabilities?

• Compliance Infrastructure: Does the Compliance Officer have sufficient authority to implement the compliance program? Has management provided the Compliance Officer with the autonomy and sufficient resources necessary to perform assessments and respond appropriately to misconduct? Have compliance-related responsibilities been assigned across the appropriate levels of the organization? Are employees held accountable for meeting these compliance-related objectives during performance reviews?

• Measures to Prevent Violations: What is the scope of compliance-related education and training across the organization? Has the effectiveness of such training been assessed? What policies/measures have been developed to enforce training requirements and to provide remedial training as warranted? What processes are in place to ensure that appropriate remedial measures are taken in response to identified weaknesses?

• Measures to Respond to Violations: What is the process by which the organization evaluates and responds to suspected compliance violations? How are reporting systems, such as the compliance hotline, monitored to verify appropriate resolution of reported matters? Does the organization have policies that address the appropriate protection of "whistleblowers" and those accused of misconduct? What is the process by which the organization evaluates and responds to suspected compliance violations? What policies address the protection of employees and the preservation of relevant documents and information? What policies govern the reporting to government authorities of probable violations of law?

To address these and other program-specific[43] compliance issues, internal auditing and monitoring, and independent assessments of corporate compliance policies are critically important. These tools can identify errors and potential misconduct and minimize the application of the discretionary factors that would weigh in factor of criminal prosecution and related exclusion. Finally, should criminal prosecution arise, great care must be given to the agreed-upon facts contained in any corporate or individual plea agreement, as *Friedman*/Purdue Frederick instructs.

[1] FDA Regulatory Procedures Manual (RPM) Section 6-5-3, amended Jan. 26, 2011, *available at* <http://www.fda.gov/ICECI/ComplianceManuals/RegulatoryProceduresManual/ucm2005380.htm>.

[2] Emphasis added.

[3] Office of Inspector General: U.S. Department of Health & Human Services, Exclusions Program Information, *available at* <http://oig.hhs.gov/fraud/exclusions.asp>.

[4] OIG provides the following link to review the length of exclusions by subsection under Section 1128(b): <http://oig.hhs.gov/fraud/exclusions/authorities.asp>.

[5] *See* 42 C.F.R. § 1001.1901. Even beyond the prohibitions against any federal health program payments, the practical effect of an exclusion on an individual is to disable the excluded individual from his or her profession — often characterized as a "career death sentence."

[6] Lewis Morris, Chief Counsel to the Inspector General, U.S. Department of Health & Human Services, testimony before the Subcommittee on Oversight of the United States House Ways and Means Committee on Improving Efforts to Combat Healthcare Fraud (Mar. 2, 2011), *available at* <http://oig.hhs.gov/testimony.asp>.

[7] Morris Testimony at 3.

[8] *Id.* at 6.

[9] *Id.*

[10] Codified at 42 U.S.C. § 1320a-7.

[11] *See* 42 U.S.C. § 1320a-7 for the full statutory language for these categories.

[12] U.S. Department of Health & Human Services, Office of the Inspector General, Guidance for Implementing Permissive Exclusion Authority Under Section 1128(b)(15) of the Social Security Act, *available at* <http://oig.hhs.gov/fraud/exclusions.asp>, (last accessed May 24, 2011).

[13] Section 1128(b)(15)(A)(i).

[14] Section 1128(b)(15)(A)(ii). Sec. 1126(b) states that "[f]or the purposes of this section, the term 'managing employee' means, with respect to an entity, an individual, including a general manager, business manager, administrator, and director, who exercises operational or managerial control over the entity, or who directly or indirectly conducts the day-to-day operations of the entity." [Codified at 42 U.S.C. § 1320a–5].

[15] Guidance at 1.

[16] *Id.* at 3.

[17] *Id.* "[F]or example, OIG will consider the conduct alleged by the Government in a civil False Claims Act settlement with a corporate parent of the convicted or excluded entity. As used in the following factors, the term "misconduct" includes the factual basis for the criminal conviction or exclusion that underlies the potential 1128(b)(15) exclusion as well as any other conduct OIG considers relevant, including allegations in criminal, civil, and administrative matters involving the convicted or excluded entity or any related entity."

[18] *Id.*

[19] *Friedman*, 755 F.Supp.2d at 100-01.

[20] *Id.*

[21] *Id.*

[22] *Id.* at 101.

[23] *Id.* at 102.

[24] *Id.* Citing *United States v. Purdue Frederick Co.*, 495 F.Supp.2d 569 (W.D. Va. 2007).

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *See id.* at 102-03.

[29] *Id.* at 104.

[30] *Id.* at 105.

[31] *Id.* at 106-07.

[32] *Id.* at 107-08.

[33] *Id.* at 110-13.

[34] Daniel Levinson, Inspector General, U.S. Department of Health & Human Services, Testimony before the United States Senate Committee on Finance (Mar. 2, 2011), *available at* <http://oig.hhs.gov/testimony.asp>, (last accessed May 24, 2011).

[35] Alicia Mundy, *U.S. Effort to Remove Drug CEO Jolts Firms*, *Wall Street Journal*, Apr. 26, 2011, at A1.

[36] 2010 U.S. Dept. of Health & Human Services & U.S. Dept. of Justice Ann. Rep. at 1, *available at* <http://www.oig.hhs.gov/publications/docs/hcfac/hcfacreport2010.pdf>, (last accessed May 24, 2011).

[37] Annual Report at 1.

[38] *Id.* at 69.

[39] *Id.*

[40] *Id.*

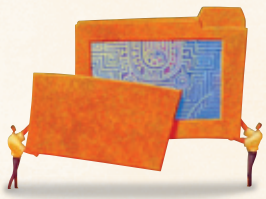
[41] *Id.* at 70.

[42] Office of Inspector General & the American Health Lawyers Association, Corporate Responsibility and Corporate Compliance: A Resource for Health Care Boards of Directors (Apr. 2003), *available at* <http://oig.hhs.gov/fraud/docs/complianceguidance/040203CorpRespRsceGuide.pdf>, (last accessed May 24, 2011).

[43] *See also* U.S. Department of Health & Human Services, Office of Inspector General, Compliance Program Guidance for Pharmaceutical Manufacturers, 68 Fed. Reg. 23731 (May 5, 2003).

WRITTEN *by* RICHELLE KIDDER

IN AN E-ERA OF ANYTHING'S ACCESSIBLE



STATE SECURITY BREACH NOTIFICATION LAWS

Enhance the Protection of Personal Information

Overview

While the talk of 2011 may be the possibility of Congressional action on a privacy bill or a single, preemptive federal data security law, states currently provide the best means of protecting personal information. Forty-six states, the District of Columbia, the District of Puerto Rico, and the Virgin Islands have enacted laws requiring organizations that possess sensitive personal information to notify individuals of privacy breaches.[1]

With California paving the way,[2] breach notification laws are driven by concerns that privacy breaches may lead to identity theft and fraud. Technological advancements have made it possible for organizations to store vast amounts of personal data electronically. Any breach of e-storage containing personal identifying information creates the risk of an unauthorized person stealing the information to assume another's identity and engage in fraud.

According to the Privacy Rights Clearinghouse, there have been more than 533 million breaches of sensitive personal information since 2005.[3] While further study is needed on information security practices, privacy breaches, and the link between these breaches and fraud, state notification statutes have motivated organizations to improve data security of personal information so as to avoid adverse publicity, embarrassment, brand damage, and the potential legal ramifications arising from the theft or misuse of personal information.[4]

Breach notification statutes apply to state and private organizations, such as data brokers, retailers, credit card issuers, payment processors, banks, furnishers of credit reports, and any other organizations that possess databanks of personal information.[5] State involvement in data breaches also has extended into the medical realm, as states enforce the Health Information Technology for Economic and Clinical Health (HITECH) Act.[6]

Security breach notification statutes generally include the following commonalities. First, the statute defines the scope and nature of the information covered by the law. Second, the statute specifies events and conditions triggering obligations under the law. Third, the statute defines obligations under the law in the event action is required. Although common attributes of breach notification statutes are discussed

below, organizations must recognize that the laws vary by state and sometimes in significant ways. If your organization experiences a data breach involving individuals in more than one state, then your obligation in different states may vary and require cumulative and concurrent action.

Scope and Nature of Information Covered by Statute

Identity theft and well-publicized data breaches prompted California to enact the first state-level security breach notification law. The California statute, which has been amended since 2003, requires any agency, person, or business that conducts business in California and "that owns or licenses computerized data that includes personal information" to notify affected California residents of any security breach in the resident's personal information that was, or is reasonably believed to have been, accessed by an unauthorized person.[7]

Under the revised California statute,[8] personal information refers to "an individual's first name or first initial and last name in combination with any one or more of the following": (a) a social security number; (b) driver's license of California identification card number; (c) account, credit, or debit card number in combination with any security or access code or password that would allow access to an individual's financial account; (d) medical information[9]; and (e) health insurance information.[10] The term "personal information," however does not include "publicly available information that is lawfully made available to the general public from federal, state, or local government records.[11]

All but four states have enacted similar data breach notification laws.[12] Mississippi enacted the most recent statute, which takes effect on July 1, 2011.[13] Some states have more expansive definitions of "personal information" so as to the name of the person (first name or initial and last name) plus email address, alien registration number, passport number, employer or tax ID number, Medicaid or food stamp account number, biometric data and fingerprints, insurance policy number, Department of Transportation operator's number, unique electronic number, address, or routing code.[14]

New York's statute takes a different approach. Instead of using the name of the person, it defines "personal information" as "any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person."[15] It then defines "private information" as "personal information in combination with any one or more of the following data elements [such as social security number, driver's license, etc.]" when "either the personal information or the data is not encrypted, or encrypted with an encryption key that has also been acquired[.]"[16]

> *While the talk of 2011 may be the possibility of Congressional action on a privacy bill or a single, preemptive federal data security law, states currently provide the best means of protecting personal information.*

In the vast majority of states, the application of breach notification laws is limited to computerized data that contains personal information, and even then, only if the computerized data is unencrypted. Some statutes, such as Maine, North Carolina, Ohio, and Pennsylvania, define the term "encrypted," while others, such as California, do not. In a small number of states, breach notification obligations may be implicated if personal information in paper records is the subject of a breach.

Lastly, some states, such as Illinois, Ohio, and Pennsylvania, exempt redacted information from notification obligations. The term "redacted" is not always defined, which provides uncertainty as to what type or extent of redaction eliminates the notification requirement.

Events and Conditions Triggering Breach Notification Obligations

Breach notification laws typically apply if "personal information" is acquired by an unauthorized person or in the event that there is a breach of the security of the system. A "breach" is considered to have occurred when someone acquires computerized data that compromises the security, confidentiality, or integrity of personal information. Some issues to consider are whether "acquired" is the same as "accessed." Further, some statutes cover an acquisition that compromises the "integrity" of personal information.

As we all know from high-tech law enforcement shows like *Criminal Minds* and *NCIS*, discovering a breach of security may be difficult. Skilled hackers like characters Penelope Garcia or Timothy McGee can erase their steps in the electronic storage system. They can disguise the destination of downloaded data. Accordingly, in some instances, identifying the security breach that triggers the notification obligations may present challenges, but the organization cannot merely rely on the absence of evidence. To quote from the Global Practices — Consumer Protection and Data Breach Notification Conference, "[t]he absence of evidence is not evidence of absence."[17]

Some statutes require notification whenever there is unauthorized access of personal information, while others do not require notification if an organization reasonably determines that harm is not likely to result from the breach. New York's statute takes it further and requires that companies notify the Attorney General, the Consumer Protection Board, and the State Officer of Cyber Security and Infrastructure Coordination about the number of individuals affected and the timing and distribution of the notice.[18] All state notification breach statutes place the burden for deciding whether notification is required on the organization itself.

Most statutes provide some flexibility concerning the type of notice that must be provided. Written notice is the standard approach, with many states allowing electronic notice if such notice is provided in a manner consistent with the Electronic Signatures in Global and National Commerce Act (E-SIGN Act).

When and What Type of Notice is Required?

If an organization determines that a breach requiring notice has occurred, a myriad of issues arise, the most complex being when and what type of notice must be given to the individual whose personal information has been compromised. In general, notice must be given as expeditiously as possible without unreasonable delay, although notice may be delayed if providing notice would interfere with a law enforcement investigation. A few states have bright line rules setting forth a specific number of days within which notice must be provided.

Notwithstanding, most statutes provide some flexibility concerning the type of notice that must be provided. Written notice is the standard approach, with many states allowing electronic notice if such notice is provided in a manner consistent with the Electronic Signatures in Global and National Commerce Act (E-SIGN Act). A few states permit telephonic notice.

Under certain circumstances, such as breaches involving an unusually large number of individuals or where costs of notification may be beyond the resources of a small business, substitute notice is permitted. Substitute notice generally requires email notice of possible, conspicuous posting of notice on a company's website, and notification to a major statewide media outlet. A few states require that notice must be given to state authorities in addition to those individuals whose information was the subject of a breach.

Most state statutes do not specify exactly what must be stated in the notice; however, the states that do, serve as useful guidance. Generally, they provide that notice must describe the breach incident, the type of personal information that was placed at risk, and the steps that the company has taken to minimize or prevent further risk. It is also commonly required that the notice should include a telephone number that the individual can call with questions or to seek further guidance, as well as a reminder that individuals should exercise diligence in monitoring their accounts and finances such as credit reports to determine whether the breach has resulted in any specific harm.

Practical Steps

Organizations must be proactive in the management and security of personal information stored on electronic systems and should implement an offensive notification plan. Based on studies conducted by the Samuelson Law, Technology, & Public Policy Clinic,[19] components to consider in developing a plan include:

- A uniform standard that requires public notice of all personal information breaches, which serves to ensure that all affected consumers are being provided with breach notices;
- A uniform reporting standard, which requires notification to a centralized organization in addition to consumers.
- Clarify and broaden technology safe harbor provisions beyond encryption, which serves to give better guidance to the organization on what types of security mechanisms are sufficient to prevent lost data from being accessible for the purpose of misuse.
- Create a safe harbor period for notifications, which serves to balance the need to give clear instructions on how quickly notifications must be given with the need to provide flexibility for the organization to investigate and remedy security breaches.
- Collect information on the type of notification trigger that should be used.

Some statutes require notification whenever there is unauthorized access of personal information, while others do not require notification if an organization reasonably determines that harm is not likely to result from the breach.

The following statutes require companies to notify consumers when their personal information has been breached:

Alaska: Alaska Stat. § 45.48.010 et seq. Notification may be via written notice or by electronic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. Penalty: Up to $500 per resident who was not notified.

Arizona: Ariz. Rev. Stat. § 44-7501. Notification may be via written notice or by electronic or telephonic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. Penalty: Up to $10,000 per breach.

Arkansas: Ark. Code § 4-110-101 et seq. Notification may be via written notice or by electronic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available.

California: Cal. Civ. Code §§ 1798.29, 1798.82. Notification may be via written notice or by electronic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available.

Colorado: Colo. Rev. Stat. § 6-1-716. Notification may be via written notice or by electronic or telephonic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available.

Connecticut: Conn. Gen Stat. 36a-701(b). Notification may be via written notice or by electronic or telephonic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available.

Delaware: Del. Code tit. 6, § 12B-101 et seq. Notification may be via written notice or by electronic or telephonic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available.

Florida: Fla. Stat. § 817.5681. Notification may be via written notice or by electronic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. Penalty: Up to $500,000 for failure to notify within 45 days.

Georgia: Ga. Code §§ 10-1-911, -912. Notification may be via written notice or by electronic or telephonic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available.

Hawaii: Haw. Rev. Stat. § 487N-2. Notification may be via written notice or by electronic or telephonic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. See statute for specific notice requirements. Penalty: Up to $2,500 for each violation plus damages incurred as a result of the breach.

Idaho: Idaho Stat. §§ 28-51-104 to 28-51-107. Notification may be via written notice or by electronic or telephonic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. Penalty: Up to $25,000 per breach.

Illinois: 815 ILCS 530/1 et seq. Notification may be via written notice or by electronic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available.

Indiana: Ind. Code §§ 24-4.9-1-1 et seq., 4-1-11 et seq. Notification may be via written notice, facsimile, or by electronic or telephonic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. Penalty: Up to $150,000 and cost for attorney general to enforce.

Iowa: Iowa Code § 715C.1. Notification may be via written notice or by electronic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. See statute for specific notice requirements.

Kansas: Kan. Stat. 50-7a01, 50-7a02. Notification may be via written notice or by electronic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available.

Louisiana: La. Rev. Stat. § 51:3071 et seq. Notification may be via written notice or by electronic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. Penalty: Actual damages caused by breach.

Maine: Me. Rev. Stat. tit. 10 §§ 1347 et seq. Notification may be via written notice or by electronic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. Business shall also notify the appropriate state regulators within the Department of Professional and Financial Regulation, or if the person is not regulated by the department, the Attorney General. Penalty: Up to $500 per violation; maximum of $2,500 for each day the business is in violation.

Maryland: Md. Code, Com. Law § 14-3504 et seq. Notification may be via written notice or by electronic or telephonic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. See statute for specific notice requirements. A business shall provide notice of a breach to the Office of the Attorney General prior to giving the notification.

Massachusetts: Mass. Gen. Laws 93H § 1 et seq. Notification may be via written notice or by electronic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. The notice shall also be provided to the attorney general and consumer reporting agencies or state agencies, if any. See statute for specific notice requirements.

Michigan: Mich. Comp. Laws § 445.72. Notification may be via written notice or by electronic or telephonic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. See statute for specific notice requirements. Penalty: Up to $250.00 for each failure to provide notice, not to exceed $750,000.

Minnesota: Minn. Stat. §§ 325E.61, 325E.64. Notification may be via written notice or by electronic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available.

Mississippi: Miss. Code Ann. § 75-24-29 (eff. July 1, 2011). Notification may be via written notice or by electronic or telephonic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available.

Missouri: Mo. Rev. Stat. § 407.1500. Notification may be via written notice or by electronic or telephonic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. See statute for specific notice requirements. In the event a business provides notice to more than one thousand consumers at one time, the business shall notify the attorney general's office.

Montana: MCA §§ 30-14-1704, 2-6-504. Notification may be via written notice or by electronic or telephonic means. Where a large breach occurs or where the cost to

notify is high, alternative methods of notice are available.

Nebraska: Neb. Rev. Stat. §§ 87-801 et seq. Notification may be via written notice or by electronic or telephonic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available.

Nevada: Nev. Rev. Stat. 603A.010 et seq. Notification may be via written notice or by electronic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available.

New Hampshire: N.H. Rev. Stat. §§ 359-C:19, -C:20, -C:21. Notification may be via written notice or by electronic or telephonic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. See statute for specific notice requirements.

New Jersey: N.J. Stat. 56:8-163. Notification may be via written notice or by electronic or telephonic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. The breach of security and any information pertaining to the breach must be reported to the Division of State Police in the Department of Law and Public Safety before notification to the customer.

New York: N.Y. Gen. Bus. Law § 899-aa. Notification may be via written notice or by electronic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. Business shall notify the state attorney general, the consumer protection board, and the State Office of Cyber Security and Critical Infrastructure Coordination as to the timing, content, and distribution of the notices and approximate number of affected persons.

North Carolina: N.C. Gen. Stat § 75-65. Notification may be via written notice or by electronic or telephonic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. See statute for specific notice requirements. The business shall notify without unreasonable delay the Consumer Protection Division of the Attorney General's Office of the nature of the breach, the number of consumers affected by the breach, steps taken to investigate the breach, steps taken to prevent a similar breach in the future, and information regarding the timing, distribution, and content of the notice.

State involvement in data breaches also has extended into the medical realm, as states enforce the Health Information Technology for Economic and Clinical Health (HITECH) Act.

North Dakota: N.D. Cent. Code § 51-30-01 et seq. Notification may be via written notice or by electronic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available.

Ohio: Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192. Notification may be via written notice or by electronic or telephonic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. Penalty: Up to $1,000 a day for violations. After 60 days, $5,000 a day penalty. After 90 days, a $10,000 a day penalty.

Oklahoma: OK ST. T. 74 § 3113.1 and 24 § 161 to -166. Notification may be via written notice or by electronic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. Penalty: Up to $150,000.00 per breach or actual damages.

Oregon: Oregon Rev. Stat. § 646A.600 et seq. Notification may be via written notice or by electronic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. See statute for specific notice requirements.

Pennsylvania: 73 Pa. Stat. § 2303 et seq. Notification may be via written notice or by electronic or telephonic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available.

Rhode Island: R.I. Gen. Laws § 11-49.2-1 et seq. Notification may be via written notice or by electronic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. Penalty: Up to $100 per occurrence, not to exceed $25,000.

South Carolina: S.C. Code § 39-1-90. Notification may be via written notice or by electronic or telephonic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. Penalty: Up to $1,000 for each resident whose information was accessible by reason of the breach (amount to be decided by the Department of Consumer Affairs).

Tennessee: Tenn. Code § 47-18-2107, 2010 S.B. 2793. Notification may be via written notice or by electronic or telephonic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available.

Texas: Tex. Bus. & Com. Code § 521.053. Notification may be via written notice or by electronic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available.

Utah: Utah Code §§ 13-44-101, -102, -201, -202, -301. Notification may be via written notice or by electronic or telephonic means.

Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. Penalty: Up to $2,500 for a violation or series of violations concerning a specific consumer; and no greater than $100,000 in the aggregate for related violations concerning more than one consumer.

Vermont: 9 V.S.A. § 2430 et seq. Notification may be via written notice or by electronic or telephonic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. See statute for specific notice requirements.

Virginia: Va. Code § 18.2-186.6, § 32.1-127.1:05 (effective January 1, 2011). Notification may be via written notice or by electronic or telephonic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. See statute for specific notice requirements. Business shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to the Office of the Attorney General.

Washington: Wash. Rev. Code § 19.255.010, 42.56.590. Notification may be via written notice or by electronic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available.

West Virginia: W. Va. Code §§ 46A-2A-101 et seq. Notification may be via written notice or by electronic or telephonic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. See statute for specific notice requirements. No civil penalty unless repeated and willful violations. Penalty: Up to $150,000.

Wisconsin: Wis. Stat. § 134.98 et seq. Notification may be via mail or by a method the business has previously employed to communicate with the subject of the personal information. See statute for specific notice requirements.

Wyoming: Wyo. Stat. § 40-12-501 to -502. Notification may be via written notice or by electronic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. See statute for specific notice requirements.

District of Columbia: D.C. Code § 28-3851 et seq. Notification may be via written notice or by electronic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. See statute for specific notice requirements. Penalty: Up to $100 for each violation, the costs of the action, and reasonable attorney's fees. Each failure to provide a District of Columbia resident with notification constitutes a separate violation.

Puerto Rico: PR ST T. 10 § 4051 et. seq. Notification may be via written notice or by electronic means. Where a large breach occurs or where the cost to notify is high, alternative methods of notice are available. Within a non-extendable term of ten (10) days after the violation of the system's security has been detected, the parties responsible shall inform the Department of Consumer Affairs.

[1] A state-by-state survey can be found at the end of this article.

[2] Cal. Civ. Code §§ 1798.29, 1798.82.

[3] "*500 Million Sensitive Records Breached Since 2005*," Privacy Rights Clearinghouse, Aug. 10, 2010, <http://www.privacy rights.org/500-million-records-breached> (last accessed May 5, 2011); *see also Chronology of Data Breaches*, Privacy Rights Clearing House, May 6, 2011, <http://www.privacyrights.org/data-breach#1> (last accessed May 7, 2011).

[4] See M. Turner, *Towards a Rational Personal Data Breach Notification Regime*, Information Policy Institute, at 2 (2006), <http://perc.net/files/downloads/data_breach.pdf> (last accessed May 7, 2011).

[5] *See supra* note 1.

[6] In February 2009, President Obama signed the HITECH Act as part of his overall economic stimulus plan. 42 U.S.C. §§ 300jj-15, 300jj-16, 300jj-17(d) (2010). The HITECH Act continues the effort of the Health Insurance Portability and Accountability Act (HIPAA) to encourage movement to electronic patient records and to deliver stricter data protection regulations for more secure patient privacy. *Id.* Among the most important of the HITECH Act mandates is a federal breach notification requirement for stored health information that is not encrypted or otherwise made indecipherable, as well as increasing penalties for violations. *Id.* Until this law was passed, only two of the 46 states with data breach notification requirements included health information as a specified data type. *Id.*

[7] Cal. Civ. Code § 1798.82.

[8] *Id.* at §1798.82(e).

[9] "Medical information" means "any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health-care professional." *Id.* at §1798.82 (f)(2).

[10] "Health insurance information" means "an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records." *Id.* at §1798.82 (f)(3).

[11] *Id.* at §1798.82 (f)(1).

[12] States with no security breach notification laws: Alabama, Kentucky, New Mexico, and South Dakota.

[13] The law, which will take effect July 1, 2011, applies to the unauthorized acquisition of unencrypted electronic files, media, databases, or computerized data containing personal information of any Mississippi resident. See Miss. Code §75-24-29. The law contains a harm threshold specifying that notification is not required if it can be reasonably determined that the breach will not likely result in harm to affected individuals. *Id.* at ¶ 7. The statute on its face does not recognize a private cause of action. *Id.* at ¶ 8.

[14] For a more comprehensive discussion on different state notification of breach statute see *Canadian Internet Policy and Public Interest Clinic, Approaches to Security Breach Notification: A White Paper*, 11-14 (2007), <http://www.cippic.ca/uploads/BreachNotification_9jan07-print.pdf> (last accessed on May 2, 2011).

[15] N.Y. Gen. Bus. Law § 899-aa(1)(a) (2005).

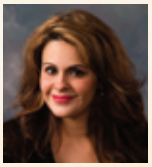
[16] *Id.* at § 899-aa(1)(b).

[17] *See Global Practices — Consumer Protection and Data Breach Notification, Nov. 14, 2007*, <http://apps.americanbar.org/buslaw/newsletter/0067/materials/pp2.pdf at 14> (last accessed May 7, 2011).

[18] N.Y. Gen. Bus. Law § 899-aa(8)(a).

[19] Samuelson Law, Technology & Public Policy Clinic, "Security Breach Notification Laws: Views from Chief Security Officers." Technical report, University of California, Berkeley, December 2007, <http://www.law.berkeley.edu/files/cso_study.pdf> (last accessed May 7, 2011).

Written *by*
Anita Modak-Truran
and Katie Bryant




Health Insurance Portability
and Accountability Act
of 1996
ADMINISTRATIVE REQUIREMENTS
Privacy Policies and Procedures.
A covered entity must develop
and implement written
privacy policies and
procedures that are
consistent with the
Privacy Rule.

Coming Soon:

HIPAA

gets a

FACELIFT

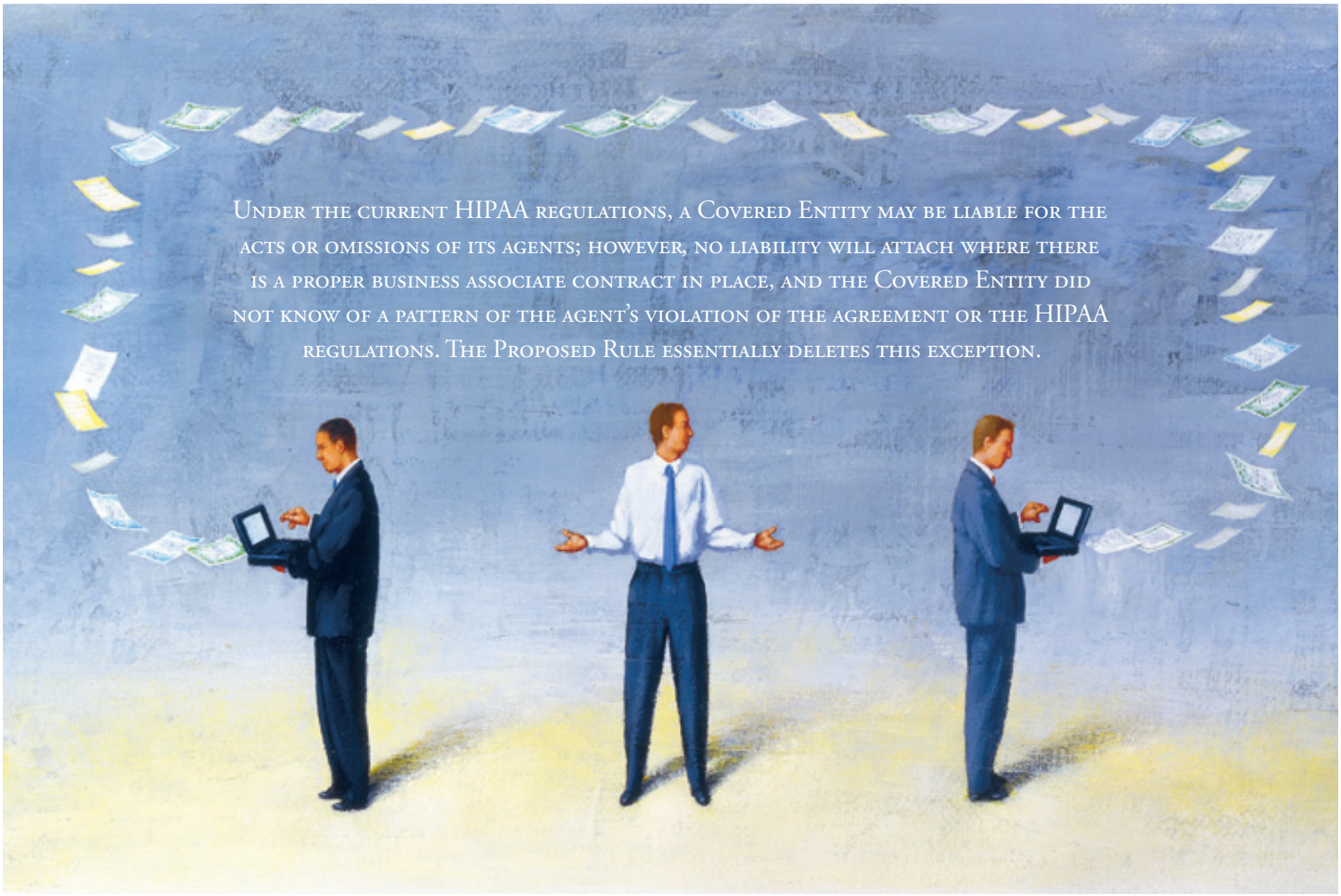
Over the past several years, the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[1] has been one of the most significant mediums by which federal law governs how healthcare providers, health plans and healthcare clearinghouses ("Covered Entities") use and disclose individually identifiable health information (known as "protected health information" or "PHI"). In 2009, the Health Information and Technology for Economic and Clinical Health Act (HITECH), a component of the American Recovery and Reinvestment Act of 2009,[2] reconfigured key components of HIPAA, such that the original law has acquired several new features.

HITECH requires HIPAA to undergo extensive remodeling in several of its primary regulations: 1) revised Privacy Rule[3] and Security Rule[4] provisions; 2) revised Enforcement Rule Provisions[5]; and 3) an added Breach Notification rule.[6] Although HITECH drew a general sketch for how these features will apply to Covered Entities and those persons or businesses performing services on their behalf ("Business Associates"), the Department of Health and Human Services (DHHS) is scheduled to further structure and define these new aspects of HIPAA. DHHS has yet to publish its final rule, but a proposed rule published in July 2010 provides a few hints as to what we can expect in the final HIPAA regulations.

1. Compliance Date. DHHS recognized that compliance with the HITECH statutory provisions would be difficult until after the final rule establishes the revised HIPAA regulations. As a solution, DHHS has proposed that Covered Entities and Business Associates will have 180 days after the effective date of the final HIPAA rule to bring their business practices in compliance. Further, DHHS has proposed that all future changes to HIPAA will follow this pattern — compliance necessary 180 days after the effective date of any final rule.

2. Expansion of the Definition of Business Associate. The Proposed Rule includes several additions to the definition of *Business Associate*. These additions include certain Patient Safety Organizations, Health Information Organizations, E-Prescribing Gateways and any subcontractors of otherwise defined Business Associates. Of these, the addition of Business Associates' subcontractors presents a marked change. Under the Proposed Rule, Business Associates have the burden to ensure appropriate business associates agreements are in place with any person or entity acting on behalf of the Business Associate with respect to the Covered Entity's PHI, other than in a capacity as a member of the Business Associate's workforce. DHHS has explained that this definition encompasses any "agent" of a Business Associate, whether or not that agent has entered into a business associate agreement with the Business Associate.

3. Liability for Agents. Under the current HIPAA regulations, a Covered Entity may be liable for the acts or omissions of its agents; however, no liability will attach where there is a proper business associate contract in place, and the Covered Entity did not know of a pattern of the agent's violation of the agreement or the HIPAA regulations. The Proposed Rule essentially deletes this exception and renders the Covered Entity liable for the actions of its agents,



including workforce members or subcontractors, who act within the scope of their agency and violate HIPAA by failing to perform an obligation on the Covered Entity's behalf. Furthermore, the Proposed Rule adds a provision that includes Business Associates' liability for their agents as well and in the same manner as liability extends for Covered Entities on behalf of their agents.

4. Transition Provision for Business Associates Agreements. DHHS stated in the Proposed Rule that it recognizes that Covered Entities may be unduly burdened by the obligation to renegotiate their business associates agreements in time to bring these in line with HITECH and the impending HIPAA revisions, especially those agreements that are not scheduled to expire or renew until after the compliance period for the new HIPAA regulations has lapsed. For this reason, DHHS has proposed that all existing business associates agreements between Covered Entities and Business Associates and between Business Associates and their subcontractors may remain in place for a period up to one year after the compliance date of the final rule, so long as the existing contract complies with HIPAA and is not renewed or modified until after the compliance date. However, DHHS also specifically stated that this transition provision only applies to amending current business associates agreements — it does not apply to the obligation for all business associates to actually be in compliance as of the compliance date.

The Proposed Rule makes several other significant changes to HIPAA, including expansion of many of the Security Rule's provisions to Business Associates (and their subcontractors), and several key changes to the Privacy Rule such as new regulations governing ways in which Covered Entities may use PHI in their marketing, fundraising, and research; the rights of individuals with respect to their PHI; and the ways in which Covered Entities provide notice to individuals about uses and disclosures of PHI.

When DHHS publishes the final rule, we will provide an in-depth analysis of the HIPAA revisions, along with a discussion of the practical effect for Covered Entities and Business Associates and what these groups can do to be prepared for the final compliance date.

[1] 45 CFR Parts 160, 162, and 164.

[2] Pub. L. 111-5 (Feb. 17, 2009).

[3] 45 CFR § 160, 164, Subparts A and E. The Privacy Rule deals with privacy standards for all protected electronic health information.

[4] 45 CFR § 160, 164, Subparts A and C. The Security Rule deals with the security standards for electronic protected health information.

[5] 45 CFR § 160, Subparts C, D, and E.

[6] 45 CFR § 164, Subpart D. Certain changes are expected to have the greatest impact.

Written *by* Shannon Hoffert

Team Members

Robert G. "Bob" Anderson
Cara R. Baer
M. Melissa Baltz
Amanda B. Barbour
P. Ryan Beckett
Al Bright, Jr.
Michael L. Brown
Denise D. Burke
Donald Clark, Jr.
Kimberly S. Coggin
Charles R. Crawford
John A. "Jack" Crawford, Jr.
Mark A. Dreher
William M. Gage
Mark W. Garriga
Hemant Gupta
Charles C. Harrell
Michael B. Hewes
Shannon E. Hoffert
Eric E. Hudson
Chad R. Hutchinson
Donna Brown Jacobs
David P. Jaqua
Alyson Bustamante Jones
Richelle W. Kidder
James J. Lawless, Jr.
Anita Modak-Truran
Charles F. Morrow
Ashley H. Nader
Amy M. Pepke
Orlando R. Richmond, Sr.
Benjamin W. Roberson
Scott B. Shanker
Machelle D. Shields
Bart N. Sisk
Hollie A. Smith
Adam J. Spicer
Kari L. Sutherland
Ronald G. Taylor
Julie Watson Lampley
J. Paul Varner
Thomas E. Williams

For additional information, including bios and contact information, please visit us at www.butlersnow.com.

BUTLER | SNOW

www.butlersnow.com