



BNA's

HEALTH LAW REPORTER



Reproduced with permission from BNA's Health Law Reporter, Vol. 18, No. 37, 09/24/2009. Copyright © 2009 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

PRIVACY

Heightened Enforcement of Privacy and Security Laws Creates New Liability and Compliance Challenges for Providers and Business Associates

By TERESE A. MOSHER BELURIS,
BENJAMIN A. DURIE, AND AMBER GOSNEY

After an initial flurry of activity to comply with privacy and security obligations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) by the 2003 and 2005 deadlines,¹ generally lax enforcement by federal agencies over the first five years of HIPAA's existence led many providers to turn their attention away from privacy issues. As the public sought to redress their providers' lax security and resultant invasions of privacy, they found that HIPAA did not provide a private right of action and were turned

¹ The deadline for most covered entities to comply with the Privacy Rule was April 14, 2003, except for small health plans, which had a compliance deadline of April 14, 2004. The deadline for most covered entities to comply with the Security Rule was April 20, 2005, except small health plans, which had until April 20, 2006.

Mosher Beluris is a partner in the Los Angeles office of McDermott Will & Emery LLP. She is past co-chair of the Managed Care Subcommittee of the Health Law Litigation Committee. Durie is an associate in the firm's Los Angeles office. Gosney is a third-year law student at Southwestern Law School.

away by the courts. The last several years, however, have seen dramatic changes to the privacy and security landscape in the health care arena. Both the courts and legislative branches became increasingly reluctant to leave individuals without redress. New federal and state legislation, a recent centralization of the federal enforcement framework, and a reinvigorated public interest in the privacy and security of medical records, in particular, demonstrate renewed focus on privacy and security compliance by providers.

In February, Congress passed the American Recovery and Reinvestment Act of 2009 (ARRA),² which included the Health Information Technology for Economic and Clinical Health Act (HITECH Act).³ The HITECH Act established a much more robust regulatory framework for the security and privacy provisions of HIPAA⁴ and provided a mandate for improved enforcement by the Department of Health and Human Services (HHS). Pursuant to this authority, on Aug. 4, HHS centralized the enforcement of the Privacy and Security rules and pledged to significantly increase federal enforcement.

² American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009).

³ American Recovery and Reinvestment Act of 2009, Health Information Technology for Economic and Clinical Health Act (HITECH Act), § 13001, et seq. (Feb. 17, 2009).

⁴ Title XIII of Division A and Title IV of Division B of the act are known as the "Health Information Technology for Economic and Clinical Health Act" (HITECH Act).

These actions just add weight to the already dramatic increase in federal enforcement that has taken place over the last few years.

In addition, although acts by the federal government have brought attention to HIPAA compliance over the last six months, in reality they just add detail to an ever-expanding patchwork of federal and state privacy laws protecting patient information. The vast majority of states have their own set of privacy and security laws and in recent years states such as California, Massachusetts, and New York have responded to high profile cases involving the disclosure of patient information by expanding their privacy laws and security rules even further.

These efforts and legislative changes require careful scrutiny of existing policies and business procedures as both individuals and companies face mounting health care liabilities. This article attempts to provide a roadmap for not only the new challenges posed by HITECH and new state laws but also the enduring challenges posed by the original privacy and security obligations created by HIPAA itself.

I. Overview of HIPAA Security and Privacy Rules

In an effort to curtail rising health care costs and address public concern relating to the privacy of medical information, Congress enacted HIPAA in 1996.⁵ Pursuant to the delegation of authority in the Administrative Simplification portion of HIPAA, HHS created the Privacy Rule and Security Rule (collectively the rules).⁶ The rules originally applied to “covered entities,” including health plans, health care clearinghouses and health care providers that transmit electronic health information as standard transactions.⁷ The Privacy Rule’s central purpose is to limit the unauthorized use and disclosure of patients’ protected health information (PHI) by establishing standards for use and disclosure of electronic or nonelectronic PHI.⁸ The Security Rule, on the other hand, sets forth detailed steps that covered entities must take to protect *electronic* PHI.⁹ Both rules contain a comprehensive framework whereby the relevant enforcement agencies are provided with significant discretion to determine whether a HIPAA violation occurred.

II. HIPAA Enforcement Mechanisms

A. Civil Enforcement

Until very recently, HHS had divided the civil enforcement of the Security Rule and the Privacy Rule between two separate federal agencies. Originally, the Office of Civil Rights (OCR) was responsible for enforcing the Privacy Rule and the Office of E-Health Standards and Services (OEES), a department within the Centers for Medicare & Medicaid Services (CMS), enforced the Security Rule.¹⁰ As of Aug. 4, 2009, however, OCR now

is responsible for enforcement of *both* the Privacy Rule and the Security Rule.¹¹

The Privacy and Security Rules contain a cooperative compliance framework whereby OCR is provided with a great deal of discretion in determining whether or not there have been HIPAA violations in cases where the perpetrator did not know or with reasonable diligence would not have known that a violation occurred.¹² This is because technically a violation is broadly defined as any, “failure to comply with an administrative simplification provision.”¹³ In the context of contemplated civil monetary penalties (CMP) and ordinary compliance investigations, the enforcement agencies must first attempt to resolve any complaints or investigations informally with the covered entity before resorting to more serious actions such as issuing a determination that a violation has occurred. Even if OCR determined that a violation occurred, until the changes made to HIPAA under the HITECH Act, the CMPs available to HHS were relatively small and ranged from \$100 to \$25,000 per violation. This cooperative compliance framework may have been responsible for what some—including HHS itself—have interpreted as lax enforcement of the rules over the first few years of their existence.

However, recent statistics illuminate a significant movement toward increased enforcement by both OCR and CMS over the last few years. OCR reports that 9,280 privacy violation cases were resolved in 2008, with 1,163 of the 3,373 investigated cases requiring corrective action.¹⁴ These statistics are a marked increase from the mere 1,516 cases resolved in 2003 where only 260 of the 339 cases investigated required corrective action.¹⁵ Additionally, OCR conducted 1,161 more investigations in 2008 than in 2007.¹⁶

CMS has reported less robust enforcement results than OCR over the last several years;¹⁷ however, there are multiple indicators that enforcement of the Security Rule will soon be more in line with the Privacy Rule. In October 2008, the HHS Office of Inspector General (OIG) issued a report that sharply criticized CMS for taking “limited actions” to push security compliance and for its reliance on an inefficient complaint-driven process for uncovering security violations.¹⁸ As a result, CMS stated its intent to implement the compliance reviews recommended by the OIG and initiate audits nationwide. Additionally, CMS issued an audit checklist in

¹¹ 74 Fed. Reg. 38630 (Aug. 4, 2009).

¹² 71 Fed. Reg. 8390, 8400 (Feb. 16, 2006).

¹³ 45 C.F.R. § 160.302.

¹⁴ “Resolutions by Year & Type,” available at: www.hhs.gov/ocr/privacy/hipaa/enforcement/data/historicalnumbers.html.

¹⁵ *Id.*

¹⁶ OCR reports that 3,373 privacy violation cases total were investigated in 2008 compared to only the 2,212 total cases that were investigated in 2007. *Id.*

¹⁷ CMS reports only 428 cases as of June 2009, constituting only 86 more cases than those reported in July 2007. Only 47 of the 357 closed cases were closed via corrective action. Center for Medicaid and Medicare Services, “HIPAA Enforcement Statistics,” available at http://www.cms.hhs.gov/Enforcement/11_HIPAAEnforcementStatistics.asp.

¹⁸ Department of Health & Human Services, Office of Inspector General, “Nationwide Review of the Centers for Medicare & Medicaid Services Health Insurance Portability and Accountability Act of 1996 Oversight (A-04-07-05064)” (Oct. 2008) available at <http://oig.hhs.gov/oas/reports/region4/40705064.pdf>.

⁵ Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

⁶ Public Law 104-191, 110 Stat. 1936 (1996). The Administrative Simplification provisions of HIPAA are codified at 42 U.S.C. §§ 1320d – 1320d-8.

⁷ 45 C.F.R. § 160.103.

⁸ 45 C.F.R. § 164.102 *et seq.*

⁹ 45 C.F.R. §§ 164.308-.312 (2003).

¹⁰ See http://www.cms.hhs.gov/CMSLeadership/14_Office_OEES.asp.

2008 notifying covered entities about the type of information that CMS intended to review during their audits, which includes interviewing company executives such as the president, chief executive officer, or directors of the covered entity.¹⁹ Also, the HITECH Act for the first time imposes *mandatory* breach notification obligations on both HIPAA covered entities and business associates.²⁰ Finally, the recent centralization of enforcement authority under the OCR is viewed as an effort to improve the efficiency and effectiveness of the enforcement of the rules as a whole. Taken together, these actions by HHS likely foreshadow an intensified scrutiny of the rules in the near future.

B. Serious Criminal Implications

Although the Privacy Rule and the Security Rule are primarily enforced by OCR, criminal investigations are referred by OCR to the U.S. Department of Justice (DOJ).²¹ Under HIPAA's criminal provisions, 42 U.S.C. 1320d-6, a person is guilty of the wrongful disclosure of individually identifiable health information when they *knowingly and in violation of HIPAA*: (1) use or cause a unique health identifier to be used; (2) obtain individually identifiable health information relating to an individual; or (3) disclose individually identifiable health information to another person. There are three levels of possible sanctions available under the statute depending on the level of intent. If the offense is committed knowingly, then the offense carries a possible fine of up to \$50,000 and/or up to one year imprisonment. If the offense is committed under false pretenses, then the offense carries a possible fine up to \$100,000 and/or up to five years imprisonment. If the offense is committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, then the offense carries a possible fine up to \$250,000 and/or up to 10 years imprisonment.²² As of June, OCR has referred 459 cases to the DOJ for criminal investigation involving the knowing disclosure or obtaining of PHI in violation of the Privacy Rule.²³

The difficulty in applying the criminal elements of 1320d-6 to specific acts is that, unlike the civil enforcement mechanism, there are no clear regulations accompanying the statute. To provide greater clarity on the application of 1320d-6, the DOJ issued a memorandum in June 2005 outlining the scope of criminal enforcement.²⁴ Specifically, the DOJ discussed two central issues: (1) whether "knowingly" requires proof of knowledge of the facts that constitute the offense or whether proof of knowledge that the law was violated is re-

quired; and (2) whether individuals can be prosecuted directly under the statute.²⁵

The DOJ concluded that in order to prove that the accused individual committed the alleged act "knowingly," the government only has to show the individual had knowledge of the facts that constitute the offense. Although the DOJ argued that this position is consistent with federal case law, the practical consequences of this interpretation in the HIPAA setting are massive as it essentially creates a strict liability standard. The logical consequence of the DOJ's position is that all HIPAA violations that involve obtaining, using or disclosing PHI in violation of HIPAA would constitute criminal acts. Arguably, a large percentage of all potential HIPAA violations would fall within these categories. Such a reality would severely undermine the cooperative approach outlined in the HIPAA statute and administrative simplification regulations because covered entities would be much less willing to disclose potential violations out of fear of potential criminal prosecution.

The DOJ's position also is directly opposed to the approach Congress and HHS have taken with respect to the imposition of civil monetary penalties. The civil enforcement section provides, "no penalty may be imposed . . . if the failure to comply is corrected during the 30-day period beginning on the first date the person liable for the penalty or damages knew or by exercising reasonable diligence would have known, that the failure to comply occurred."²⁶ Therefore, civil monetary penalties cannot be imposed when individuals only had knowledge of the facts that constitute the offense and not that the act actually violated HIPAA.

At the time, the DOJ also decided that the criminal penalties for violations of HIPAA are directly applicable only to covered entities.²⁷ Applying principles of "corporate criminal liability," the DOJ warned that individuals, such as directors, employees, or officers of a covered entity, also may be criminally liable under HIPAA where the covered entity is not an individual. Charges of conspiracy in addition to aiding and abetting also are available to the DOJ in cases where an individual of a covered entity is not directly liable.²⁸ However, despite the official DOJ guidance, local U.S. attorneys actually have prosecuted individuals that were not covered entities or accountable to covered entities.²⁹ The HITECH Act attempts to provide some clarification on whether or not individuals can be prosecuted under HIPAA, although questions remain whether business associates or other third parties that may have misused health information could be prosecuted under the amended criminal standard.³⁰

Since the first HIPAA criminal prosecution that was initiated in 2005, there have only been eight criminal felony convictions with one of the most recent being a 25-year-old nurse. Despite the few actual convictions, a DOJ spokesperson reported in 2008 that department

¹⁹ Department of Health & Human Services, CMS, "Sample—Interview and Document Request for HIPAA Security Onsite Investigations and Compliance Reviews" (2008) available at <http://cms.hhs.gov/enforcement/downloads/informationrequestforcompliancereviews.pdf>.

²⁰ 42 U.S.C. § 17932.

²¹ 71 Fed. Reg. 8390 (Feb. 16, 2006).

²² 42 U.S.C. § 1320d-6.

²³ Department of Health and Human Services, "Health Information Privacy—Enforcement Highlights" available at <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html>.

²⁴ Scope of Criminal Enforcement Under 42 U.S.C. § 1320d-6, Memorandum Opinion for The General Counsel Department of Health and Human Services and The Senior Counsel to the Deputy Attorney General (June 1, 2005), available at http://www.usdoj.gov/olc/hipaa_final.htm.

²⁵ *Id.*

²⁶ 42 U.S.C. § 1320d-5(b)(2).

²⁷ Scope of Criminal Enforcement Under 42 U.S.C. § 1320d-6, Memorandum Opinion for The General Counsel Department of Health and Human Services and The Senior Counsel To the Deputy Attorney General (June 1, 2005), available at http://www.usdoj.gov/olc/hipaa_final.htm.

²⁸ *Id.*

²⁹ *United States v. Ferrer*, No. 06-cr-60261-JIC (S.D. Fla. Apr. 30, 2007).

³⁰ HITECH Act, Section 13409.

filed around 200 criminal cases since 2003 under the Social Security statute that includes HIPAA.³¹ In April 2008, the DOJ issued a press release where the U.S. attorney for the Eastern District of Arkansas, Jane Duke, conceded that criminal enforcement of HIPAA is a “fairly new concept.” However, the U.S. attorney clearly warned that covered entities can look forward to “vigorous enforcement” and “swift prosecution” for persons who violate HIPAA for personal gain or malicious harm.³²

Notwithstanding the cooperative approach built into the Security and Privacy Rules and applied by HHS during civil investigations, the 2005 DOJ position paper provides alarming clarity on the nature and scope of criminal enforcement under HIPAA. Further, the position paper illuminates the serious criminal liability for HIPAA violations and foretells of the possible shift toward strict liability for such violations.³³ Despite the attempt made by the HITECH Act to clarify the situation, questions remain as to the true scope of criminal liability under HIPAA.

C. Private Right of Action

Despite being a rule focused on the protection of individuals’ health information, the Privacy Rule creates no specific private right of action for individuals whose PHI is used or disclosed in violation of HIPAA. Instead, the enforcement agency is empowered to conduct investigations and prosecutions on behalf of individuals. Nonetheless, the HIPAA standards have crept into the courtrooms via civil lawsuits. Plaintiffs recently have utilized the federal standards to prove liability in state tort lawsuits dealing with inadequately protected medical records.³⁴ In *Acosta v. Byrum*, the North Carolina appellate court conceded that HIPAA does not explicitly provide for a private cause of action.³⁵ However, the court proceeded to allow the plaintiff to cite HIPAA as evidence of the duty of care owed by the doctor to prove a negligent infliction of emotional distress claim.³⁶ This standard was continued in *Sorenson v. Barbuto* where the Utah appellate court permitted the use of HIPAA to demonstrate the proper standard of care owed by the physician.³⁷ Although there is no specific private cause of action afforded by HIPAA, covered entities, business

associates, and vendors still may be held to HIPAA standards in civil cases.

In addition, some states endorse compliance with privacy and security laws by creating their own causes of action for security and privacy breaches under state law. For example, California authorizes consumers to enjoin a business that fails to comply with state laws that require the institution of specific safeguards to protect consumer personal information.³⁸ Many other states are likely to follow suit, giving entities and individuals dealing with personal information even more reason to take precautionary measures to ensure compliance with both federal and state privacy and security laws to avoid costly litigation.

III. New Federal Legislation

ARRA, and the HITECH Act embedded in it, are consistent with the Obama administration’s emphasis on the universal adoption of electronic health records and the implementation of a nationwide health information network. ARRA allocates \$19 billion in federal funding to accelerate the adoption and use of certified electronic health record technology. The institution of new federal privacy and security provisions has significant liability implications for health care providers, health plans, health care clearinghouse, business associates, and some vendors and service providers.

A. New Obligations Under the HITECH Act

The HITECH Act establishes new security and privacy provisions that increase the liability risk under HIPAA. The additions to the Security Rule now provide mandatory guidelines for notification to individuals affected by *unsecured* PHI breaches.³⁹ Under HIPAA, there actually was no mandatory breach notification procedure for covered entities or business associates. The new law further defines actions that constitute a breach of PHI, which include inadvertent disclosures.⁴⁰ The HITECH Act also includes temporary breach notification requirements that apply to vendors of personal health records and other noncovered entities and non-business associates that deal with personal health records, thus broadening HIPAA’s reach.⁴¹

In addition, individual privacy rights under HIPAA are expanded through the HITECH Act by requiring physicians to provide patients an accounting of disclosures of PHI made through the use of an electronic health record upon request.⁴² The HITECH Act eliminates the exception for “treatment, payment and healthcare operations” under the accounting of disclosure requirements and obligates covered entities to agree to certain PHI restriction requests by individuals if the health care provider is paid out of pocket in full.⁴³ Additionally, new privacy provisions prohibit the sale of PHI without express written authorization from the individual, except in limited circumstances that involve research or public health activities, and require all

³¹ Sarah Rubenstein, “Are Your Medical Records at Risk?: Amid Spate of Security Lapses, Health-Care Industry Weighs Privacy Against Quality Care” *Wall St. J.*, Apr. 29, 2008 available at <http://online.wsj.com/article/SB120941048217350433.html>.

³² Press Release, U.S. Department of Justice, “Nurse Pleads Guilty to HIPAA Violation” (April 11, 2008) available at http://www.usdoj.gov/usao/are/news_releases/PDFs_2008News_Releases/April/SmithLPNplea%20HIPAA%20041508.pdf.

³³ See Memorandum Opinion for The General Counsel Department of Health and Human Services and The Senior Counsel to the Deputy Attorney General (June 1, 2005), available at http://www.usdoj.gov/olc/hipaa_final.htm.

³⁴ See *Sorenson v. Barbuto*, 143 P.3d 295 (Utah Ct. App. 2006), *aff’d* 177 P.3d 614 (Utah 2008) (citing HIPAA standards in determining that a Utah doctor owed a duty of confidentiality to his patients, which allowed the case to proceed); *Acosta v. Byrum*, 638 S.E.2d 246 (N.C. Ct. App. 2006) (allowing privacy claim to proceed reliant upon standard of care HIPAA establishes for protection of patient medical records).

³⁵ *Acosta v. Byrum*, 638 S.E.2d 246, 253 (N.C. Ct. App. 2006).

³⁶ *Id.* at 253.

³⁷ *Sorenson v. Barbuto*, 143 P.3d at 299 n.2.

³⁸ See Cal. Bus. & Prof. Code § 17200.

³⁹ HITECH Act § 13402 (2009) (to be codified at 42 U.S.C. § 17932).

⁴⁰ *Id.*

⁴¹ HITECH Act § 13407 (2009) (to be codified at 42 U.S.C. § 17937).

⁴² HITECH Act § 13405(b), 13405(a) (2009) (to be codified at 42 U.S.C. § 17935).

⁴³ *Id.*

fundraising communications that are considered health care operations to provide clear and conspicuous opt-out opportunities to choose to not receive similar communications in the future.⁴⁴

B. Dramatic Changes for Business Associates

One of the most substantial changes the HITECH Act makes to HIPAA is the direct application of certain security and privacy requirements to business associates. HIPAA's reach now goes beyond covered entities, subjecting business associates to HITECH's new privacy provisions and HIPAA's Privacy Rules regarding restrictions on uses and disclosures of PHI. Importantly, HIPAA's security administrative safeguards, physical safeguards, technical safeguards, and security policies, procedures, and documentation requirements now apply directly to business associates.⁴⁵ All additional security requirements articulated in the HITECH Act also are applicable to business associates with the HITECH Act mandating integration of those rules into business associate agreements.⁴⁶ Thus, business associates now are faced with significant operational and legal consequences resulting from the extension of HIPAA security and privacy provisions.

C. Heightened Enforcement Provisions and Stiffer Civil Penalties

The HITECH Act sharpens HIPAA's teeth by amplifying the magnitude of HIPAA penalties. The HITECH Act mandates that HHS investigate complaints relating to willful neglect violations and impose penalties in accordance with the new CMP tiers. The new CMP system calculates the penalty amount based on the violator's corresponding level of intent. The system ranges from violators with no knowledge of such violation, providing fines ranging from \$100 to \$25,000 per violation, to uncorrected willful neglect violations, that carry a minimum penalty of \$50,000 and a maximum of \$1.5 million for each type of violation committed.⁴⁷ Importantly, all CMP proceeds now will be used to fund additional privacy and security enforcement by HHS in the future.

The recent federal legislation gives even greater power to agencies regulating HIPAA by providing ample funding to enhance enforcement of the rules. In addition to the CMP monetary proceeds, pursuant to ARRA provisions, the Office of the National Coordinator (ONC) submitted its Health Information Technology ARRA Implementation Plan (ONC implementation plan) in May that designates over \$24 million towards Privacy and Security Rule enforcement, including \$9.5 million for audits by OCR.⁴⁸ The ONC implementation plan further articulates that the ARRA funding for the rules will include modifications to OCR case and document management systems, training of the state attorneys general in their new enforcement role, and the

mandated audits.⁴⁹ In addition to the immediate impact of hefty penalties and extensive liability for individuals and companies that fail to comply with the amplified HIPAA standards, the new funding plan clarifies the serious reality of upcoming enforcement efforts to implement these rules.

Presenting even more challenges for covered entities and business associates is the statute's delegation of enforcement and auditing authority to state attorneys general. State attorneys general have the option to enjoin violators or receive damages of \$100 per violation, up to \$25,000, for violations of HIPAA security and privacy regulations that are not corrected within 30 days and that threaten or adversely affect any of the state's residents. States also may seek attorneys' fees and enforcement costs through judicial determination. To ensure compliance with HIPAA's privacy and security provisions and the privacy portion of the HITECH Act, HHS also provides authority to state attorneys general to audit covered entities and business associates.

IV. Patchwork of State Privacy and Security Regulation

Notwithstanding the sweeping effect of federal legislation relating to privacy and security provisions, entities and individuals also face rigorous compliance obligations imposed by state security notification laws that include harsher penalties and more stringent standards. Although such state action complicates compliance obligations for entities that do business throughout the country, the HITECH Act explicitly encourages states to enact further regulations by creating an exception to the general federal preemption rule prohibiting contradictory state for laws that relate to "the privacy of individually identifiable health information."⁵⁰ Therefore, applicable federal legislation permits states laws pertaining to health information to be more restrictive and forces individuals and entities to comply with both federal and state regulations regarding personal information.

As of May, 44 states in addition to the District of Columbia, Puerto Rico, and the Virgin Islands have enacted security breach notification laws regarding personal information.⁵¹ In the wake of the highly publicized security breaches at California hospitals involving celebrities such as Farrah Fawcett, Britney Spears, Tom Cruise, and the controversial "octomom" Nadya Suleman, media focus on privacy issues has significantly increased. California has enacted some of the most stringent disclosure and security procedure requirements in the nation. The laws apply to any business holding a California resident's personal information. In September 2008, the California legislature passed two new pieces of patient-privacy legislation that further tighten California's privacy standards, including requirements to report violations to the state and affected individual within five days of detection.⁵² The new California laws,

⁴⁴ HITECH Act § 13405, 13406 (2009).

⁴⁵ HITECH Act § 13401(a) (2009) (to be codified at 42 U.S.C. § 17931 (2009)).

⁴⁶ *Id.*

⁴⁷ 42 U.S.C. § 1320-d(5)(a).

⁴⁸ Department of Health and Human Services, Office of the National Coordinator for Health Information Technology: Health Information Technology, "American Recovery and Reinvestment Act: Improving Accountability and Information Technology Security" (May 2009) available at http://www.hhs.gov/recovery/reports/plans/onc_hit.pdf.

⁴⁹ *Id.*

⁵⁰ 42 U.S.C. § 1320d-7(a)(2)(B).

⁵¹ "Security Breach Notification Laws," National Conference of State Legislatures (2009) available at <http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx>.

⁵² Cal. Health & Safety Code § 130203; Cal. Health and Safety Code § 1280.15.

which became effective Jan. 1, require the safeguards to protect against “unauthorized access” to patient medical information, which includes internal misuse such as “snooping”⁵³ and create steep penalties of up to \$250,000 for violations by an individual or health care provider.⁵⁴

Another example of the stepped-up efforts at the state level is Massachusetts’s security laws, which are among the most aggressive in the country. The far-reaching security laws, like those in California, extend beyond state borders, applying to any person or entity that owns, licenses, stores, or maintains a Massachusetts resident’s personal information in either electronic or hard copy form.⁵⁵ The personal information component is satisfied by merely possessing a resident’s first initial and last name in addition to the resident’s Social Security number, driver’s license number or state-issued identification card number, or any financial account number.⁵⁶ Notification must be provided to the state attorney general, director of consumer affairs and business regulation, and all residents whose personal information was acquired or used.⁵⁷ Additionally, re-

cently issued regulations require that every entity owning, licensing, storing, or maintaining personal information about a Massachusetts resident institute a comprehensive written information security program, which must include an extensive computer security system with specific guidelines.⁵⁸ The expansion of both California and Massachusetts strict privacy laws highlight a state trend toward serious enforcement action beyond what exists on the federal level and force companies to contemplate state laws in addition to federal laws when assessing their compliance strategy.

V. Conclusion

The expansion of privacy and security laws and the increase in government resources and efforts toward enforcing HIPAA are likely to continue as the government seeks to promote widespread access to electronically stored health information for legitimate medical purposes. While providers’ security safeguards continue to prove to be inadequate, the increase in consumer education and awareness regarding privacy rights will only increase demands for more rigorous mechanisms for enforcement under state and federal laws, as well as for compensatory damages.

⁵³ *Id.*

⁵⁴ *Id.* ; see also Cal. Civ. Code § 56.36.

⁵⁵ 201 Mass. Code Regs. 17.01 (2009).

⁵⁶ Mass. Gen. Laws ch. 93H, § 1.

⁵⁷ *Id.*

⁵⁸ “Standards for the Protection of Personal Information of Residents of the Commonwealth,” 201 Mass. Code Regs. 17.03, 17.04 (2009).