

Caught in the Middle Between Federal and State Breach Notification Requirements

*Jon A. Neiditz, Esquire**

*Nelson Mullins Riley & Scarborough LLP
Atlanta, GA*

The federal security breach notification provisions contained in the Health Information Technology for Economic and Clinical Health (HITECH) Act and implementing regulations will cause patients, providers, regulators, and prosecutors to scrutinize not only security breach protocols but intrusion detection and other security measures to a much greater degree than previously. The nation's five years of experience with the state breach notification laws demonstrates the validity of that statement in two primary respects: first, business risks associated with notification requirements make them a larger driver of security initiatives than regulation even in highly regulated industries outside of healthcare; second, given significant differences in definitions and scope of the federal rules and previously enacted state laws, reconciling state or federal conflicts will be a constant chore and basis for disputes.

State Requirements in Relation to the HITECH Act Risk-of-Harm Controversy

The tipping point in the rush by state legislatures to enact laws requiring data breach notification to consumers was the ChoicePoint breach in early 2005.¹ ChoicePoint initially notified customers of its data breach only in California, the one jurisdiction that possessed a breach notification statute. Because of the public anger at ChoicePoint's limited disclosure, coupled with the fact that most people did not realize prior to the breach that there were entities such as ChoicePoint that possessed their personal information, the breach set off a wave of breach notification legislation resulting in more public knowledge of large data breaches that has ultimately resulted in data breach notification laws in forty-five states, the District of Columbia, Puerto Rico, and the Virgin Islands. The states that initially enacted data breach notification laws followed the California model—notification to consumers under the California law is triggered by the “unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity” of personally identifiable information, without regard to an assessment of the harm caused.²

The potential for breach notification to result in customer termination and serious brand damage has made breach notification—rather than regulatory requirements—arguably the most important driver of information security spending in the U.S. private sector from 2005 until the present.³ In 2005, studies and experiences began to emerge that indicated roughly 20% of consumers notified of a data breach involving their personally identifiable information (PHI) would immediately terminate

their relationship with the notifying entity (even if a vendor of that entity was responsible for the breach).⁴ The quality of a security program is infinitely debatable and most regulators are ill-equipped to argue with security experts, but once consumers are notified they can make an immediate judgment (to vote with their feet) and execute it instantly. In view of these risks, the business community began to introduce modifications, some adopted by state legislatures, that do not impose a notification obligation if there is: no risk of harm⁵ or material risk of harm;⁶ the personal data was not materially compromised;⁷ or there was no material risk of identity theft or fraud.⁸

A risk-of-harm threshold makes a big difference in notification obligations. On the one hand, it prevents consumers from being flooded with notifications that have little or no value and makes it easier for consumers to focus on the important incidents. On the other hand, given the business risks associated with notifications, organizations might not be incentivized to conduct an unbiased assessment of risk of harm to consumers. However, merely facing the prospect of notification and its business consequences—whether notification is required or not—has often prompted organizations to prioritize information security risk remediation.

The issue of whether a risk-of-harm threshold should be included in the federal breach provisions is being played out in a showdown between some members of Congress and the U.S. Department of Health and Human Services (HHS) over whether HHS' new breach notification rule impermissibly interprets the HITECH Act to include that prerequisite to notification obligations. The issue of whether the HHS inference of a risk-of-harm threshold departed from the statutory requirements is highlighted by the fact that the Federal Trade Commission (FTC) did not include a risk-of-harm threshold in its parallel rule interpreting the same statutory language with respect to vendors of personal health records, related entities, and their third-party suppliers. Although the two agencies coordinated on many aspects of their respective regulations, they came out at opposite ends of the spectrum on this issue. The FTC rule creates a rebuttable presumption that unauthorized access to personal information implies acquisition of that information, and unauthorized acquisition of the information triggers a notice requirement without regard to risk of harm.

Now, a group of influential House members⁹ has made its intentions regarding the language clear in a letter dated October 1, 2009, to HHS Secretary Kathleen Sebelius. The letter emphatically states:

ARRA's statutory language does not imply a harm standard. In drafting Section 13402, Committee members specifically considered and rejected such a standard due to concerns over the breadth of discretion that would be given to breaching entities, particularly with regard to determining something as subjective as harm from the release of sensitive and personal information.

The letter goes on to state that a “black and white” standard was chosen to enable consumer choices based on privacy practices and to make regulatory enforcement more effective.

Viewing the letter's arguments on a purely legal rather than policy or political grounds, the arguments in the letter appear to hold merit. The statutory language upon which HHS bases its harm-based threshold is that the unauthorized acquisition "compromises" the privacy or security of the information, but the word "compromises" was used in that way in the original California breach notification statute and many other intentionally "non-harm-based" breach notification statutes, as well as in the states that have adopted a harm-related threshold. Nine state legislatures seeking to enact a risk-of-harm threshold changed "compromises" to "materially compromises,"¹⁰ but ARRA Section 13402 makes no such choice. Moreover, in 2005 forty-seven attorneys general signed a letter to congressional leaders urging that any federal security breach notification law should include California's "compromises" language and avoid above all any risk-of-harm threshold.¹¹

However, a critical reason for retaining a risk-of-harm threshold derives from significant differences between the new federal definition of notice-triggering information and the corresponding definitions in the states. It is a problem arising from the statutory focus on all "unsecured PHI," from HHS' interpretation of "unauthorized" used in its definition of "breach," and from the potential unintended consequences of those choices.

A New Approach to Notice-Triggering Information

HITECH Act Section 13402 treated notice-triggering information in a way unlike any previous state law. All of the state laws were built on the California model, which targets financial identity theft or fraud, under which "personal information" means:

[A]n individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- (1) Social security number.
- (2) Driver's license number or California Identification Card number.
- (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.¹²

States have built on this definition, adding up to ten additional elements—for example, Arkansas and more recently California, Texas, and Missouri added medical information—but the basic structure of the definition of notice-triggering personal information in all states and other U.S. jurisdictions has remained a combination of data elements thought necessary to accomplish identity theft or fraud (financial, medical, or other). In that sense, all state breach notification laws (like most U.S. information security laws) are explicitly or implicitly based on the risk of certain types of harm. Moreover, only six states' laws explicitly cover paper breaches.¹³

The HITECH Act changed the subject matter of notice-triggering information to "unsecured PHI." Thus, it replaced discrete,

notice-triggering data elements with a very broad class of data that "could be used alone or in combination with other information to identify an individual who is a subject of the information."¹⁴ In so doing, the statute created a major challenge for rule-drafters to narrow the definition in a way that would make breach notification a useful exercise and not a constant one.

The HHS rule attempts to narrow this broad spectrum of information in two general ways before getting to its several explicit exclusions: (1) the inference of the risk-of-harm threshold from the word "compromises," and (2) the inference in its definition of "breach" that the "unauthorized acquisition, access, use, or disclosure of protected health information" can be interpreted as the "acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part [i.e., the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule]."¹⁵ The risk-of-harm threshold has received all of the attention to date, but the interpretation of "unauthorized" in the definition of "breach" deserves much more scrutiny than it has been given, in part because if the House leaders succeed in stripping the risk-of-harm threshold away, the definition of breach will be the primary conceptual structure left standing.

"Unauthorized," as in "unauthorized acquisition" or "unauthorized access" is—like "compromised"—both ubiquitous among the state breach notification statutes, and generally given much less definite meaning in the states than the HHS Interim Final Rule attempts to give it. The attractiveness of interpreting it to mean "in violation of the HIPAA Privacy Rule" is apparent, because that interpretation excludes, for the most part reasonably, broad ranges of uses and disclosures explicitly permitted by HIPAA, such as disclosures without authorizations for treatment, payment, and healthcare operations. Here is the rub: in citing the Privacy Rule, that interpretation is invoking not just a regulatory structure designed to protect data elements, but a more complex structure that moves beyond data elements to establish detailed rules for communication more generally, so that many violations will have nothing to do with security breaches.

Take the example of a marketing communication: you, the covered entity, share some PHI with a business associate that the business associate has every reason to get for treatment, payment, or healthcare operations purposes, but the business associate begins to use it, without your first knowing about it, for marketing purposes that are no longer permissible under the HITECH Act. An impermissible use of PHI has taken place under the Privacy Rule, but there has been no breach of any data elements that, if known, would lead your patients to take any action. The purpose of prompt consumer breach notification—to help consumers take prompt responsive action—has little to do with the purpose of that part of the Privacy Rule—to get you and your business associates to leave the patient alone. Granted, some patients might want you to notify them to confess that you made a mistake in disturbing them with your marketing initiative, but what is the conceptual difference between your noncompliance with the HIPAA Privacy Rule in that instance and any other sort of noncompliance for which there is no notification requirement, for example when you get a speeding ticket or violate the

antitrust laws? The purpose of prompt notification should not be confessional, but rather should be to enable the patient to take prompt action.

The purposes of the Privacy Rule, in other words, often have little to do with protecting consumers against security breaches, so defining unauthorized as a violation of the Privacy Rule opens the door to unintended consequences. Therefore, a surprise is in store for the House leaders pushing hard to remove the risk-of-harm threshold if they succeed: if the risk-of-harm threshold is removed and a different definition of unauthorized or breach is not chosen, the result will be not the robust non-harm-based breach notification law like California's that they seek, but an environment in which covered entities and business associates will be giving notice of many incidents that do not involve breaches of personal data elements at all.

One hopes that HHS and others will hold the course on the risk-of-harm threshold to avoid such meaningless disclosures. If that does not happen, two other approaches would be worthy of consideration. First, HHS could reconsider defining an "unauthorized" acquisition of PHI for purposes of security breach notification as a violation of the Privacy Rule, and start over with concepts more reasonably related to the desired breach notification benefits. Second, a tiered notification approach could be used, reserving immediate breach notification for a breach of elements or a combination of elements that could result in identity theft or fraud (such as name and social security number and other combinations explored by the states), and permitting further notification later. Such an approach might appear more satisfactory to privacy advocates and Congress because it would rely on an objective test of the elements breached rather than a subjective determination of risk of harm.

Given the clarity of the statutory language, however, practical considerations of preventing harm may not prevail. One likely outcome of that battle will exacerbate another major practical problem caused by the HITECH Act's breach notification provisions: duelling, simultaneously applicable federal and state requirements.

Nightmares of Dual Regulation

One of the biggest practical challenges for organizations subject to the HITECH breach notification rules is that the conceptual divergence between federal and state law will need to be bridged. Because the HITECH Act defers to HIPAA's preemption provisions, the only situations in which state law will be preempted are when state law contradicts federal law and is not "more stringent than" HIPAA, and is therefore more protective of privacy. An example of a state law that might be preempted is the provision of Massachusetts breach notification law that requires the omission of certain information from notices.¹⁶ An example of provisions of state law that would not be preempted would be some states' forty-five-day notification requirements¹⁷ as opposed to HITECH's sixty-day requirement.

For a glimpse of the agonizing determinations that lie ahead, however, consider a business associate that is an agent of the covered entity for purposes of federal agency law. Section

164.404(a)(2) provides that a covered entity is deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known to any person other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency). Therefore, when this business associate has reason to believe that it has suffered a breach, the covered entity's obligation is to disclose the breach to affected individuals within sixty days after the *business associate* should have discovered that breach. Therefore, not only must the covered entity worry about the intrusion detection capabilities of its vendors, but the federal sixty-day requirement may in fact be *shorter* than a state forty-five-day requirement because the former is triggered when the business associate, not the covered entity, should have known of the breach.

Most states will require a federal-state preemption analysis, with the exception of those states that specifically exempt HIPAA-covered entities from application of the breach notification requirements. For example, Arizona, Hawaii, Indiana, Michigan, Rhode Island, Vermont, and Wisconsin laws all specifically exempt entities regulated by HIPAA from their breach notification laws. As the Massachusetts statute cited above indicates, the need for the preemption analysis is not entirely obviated by the Interim Final Rule's new limitation of "contrary" to situations in which a covered entity would find it impossible to comply with both the state and federal requirements, or in which the state law "stands as an obstacle to the accomplishment and execution of the full purposes and objectives" of the breach notification provisions in the Act.

A key challenge in analyzing the application of federal versus state law is to assure that no more than one notice is sent to each individual, and that the state and federal processes can be integrated. The object in breach notification is typically to reach out to individuals in a direct and caring way—compliant notices often suffer from a somewhat bureaucratic flavor given the nature of the information that must be conveyed, so sending two notices to one individual about one breach should be avoided.

Enter the Attorneys General

The HITECH Act establishes a dual federal-state enforcement system that will generate further inconsistencies and unintended consequences. The HITECH Act authorizes state attorneys general (AGs) to bring civil actions in federal district court against individuals or entities who violate the HIPAA privacy and security standards. The statute permits enjoining further violations and imposition of damages up to \$100 per violation, capped at \$25,000 annually, for all violations of an identical requirement or prohibition. Given many AGs' eagerness to pursue actions in this area, this HITECH Act provision bears watching.

Conclusion

Compliance with the HITECH Act security breach notification rules against the backdrop of radically different state laws will all-too-easily deteriorate into a meaningless exercise providing little or no benefit to information security or to patients unless there are more sophisticated efforts than we have seen to date

to make as much sense as possible of the relationships between the two sets of requirements. In this regard, the outcome of the dialogue between the House leaders and HHS on the risk-of-harm threshold and/or other ways to fix the Interim Final Rule may have a huge impact. In any event, however, we will continue to struggle to make sense of these divergent requirements, and how they impact patients, employees, and others.

**Jon Neiditz is an Atlanta-based partner at Nelson Mullins Riley & Scarborough LLP who leads the firm's Information Management Practice, which focuses on developing and implementing cost-effective programs that address the risks, costs, and opportunities associated with electronic information—including in communications, collaboration and networking technologies, cloud computing, and e-records management.*

Jon would like to thank Mitchell Goodman, Esquire (National Vision Inc., Lawrenceville, GA), and Dan Orenstein, Esquire (Athena Health Inc., Watertown, MA), for their contributions and guidance in connection with this article.

1 See, e.g., www.ncsl.org/Default.aspx?TabId=13481.

2 CAL. CIVIL CODE § Section 1798.82(d).

3 See, e.g., the statement of Chris Hoofnagle, a senior fellow with the Berkeley Center for Law & Technology, that security breach notification laws have put data security “on the balance sheet.” Quoted in Shamus McGillicuddy, *Data breach costs rise, drive security spending*, SearchSMB.com, Nov. 15, 2006.

4 Ponemon Institute, *National Survey on Data Security Breach Notification*, Sep. 26, 2005. In that survey, only 8% of consumers who receive a security breach notification did not blame the organization that sent the notice (usually the “owner or licensee” of the information under applicable state laws), more than 40% said they might discontinue their relationship, and another 19% said that they had already done so.

5 This language appears in the breach notification statutes of Alaska, see ALASKA STAT. § 45.48.010 *et seq.* (2009); Arkansas, see ARK. CODE ANN. § 4-110-101 *et seq.* (2007); Connecticut, see CONN. GEN. STAT. § 36a-701b (2006); Florida, see FLA. STAT. § 817.5681 (2005); Hawaii, see HAW. REV. STAT. §§ 487N-1 to 4 (2007); Iowa, see IOWA CODE § 715C.1-2 (2008); North Carolina, see N.C. GEN. STAT. § 75-65 (2007); Oregon, see OR. REV. STAT. §§ 646A.600-646A.628 (2007); and South Carolina, see S.C. CODE ANN. § 39-1-90 *et seq.* (2009).

6 This language appears in the breach notification statutes of North Carolina, see N.C. GEN. STAT. § 75-60 *et seq.*; and South Carolina, see S.C. CODE ANN. § 39-1-90 *et seq.*

7 This language appears in the breach notification statutes of Arizona, see ARIZ. REV. STAT. § 44-7501 (2006); Florida, see FLA. STAT. § 817.5681; Idaho, see IDAHO CODE §§ 28-51-104-105 (2006); Nevada, see NEV. REV. STAT. § 603A.220 (2006); Ohio, see OHIO REV. CODE ANN. § 1349.19 (2007); Pennsylvania, see 73 PA. STAT. ANN. § 2301 to 2308 and 2329; South Carolina, see S.C. CODE ANN. § 39-1-90 *et seq.*; Tennessee, see TENN. CODE ANN. § 47-18-2107 (2005); and Wyoming see WYO. STAT. ANN. §§ 40-12-501 and 40-12-502 (2007).

8 This language appears in the breach notification statutes of Ohio, see OHIO REV. CODE ANN. § 1349.19; and Wisconsin, see WIS. STAT. § 134.98 (2006).

9 Representatives Waxman (D-CA), Rangel (D-NY), Dingell (D-MI), Palone (D-NJ), Stark (D-CA), and Barton (R-TX).

10 Arizona, Florida, Idaho, Nevada, Ohio, Pennsylvania, South Carolina, Tennessee, and Wyoming.

11 Letter from the National Association of Attorneys General to Majority Leader Bill Frist, Minority Leader Harry Reid (D-NV), Speaker Dennis Hastert (R-IL), and Minority Leader Nancy Pelosi (D-CA) dated Oct. 27, 2005.

12 CAL. CIVIL CODE § 1798.32(e).

13 The states whose laws explicitly include paper breaches are Alaska, see ALASKA STAT. § 45.48.090(1)(A) (definition of “breach of security”); Hawaii, see HAW. REV. STAT. §§ 487N-2(a); Indiana, see IND. CODE § 24-4.9-2(a) (2006) (definition of “breach of the security of data”); Massachusetts, see MASS. GEN. LAWS 93H

§ 1(a) (2007) (definition of “data”); North Carolina, see N.C. GEN. STAT. § 75-65(a); and Wisconsin, see WIS. STAT. § 134.98(1)(b) (definition of “personal information”).

14 45 C.F.R. § 164.514(b)(ii).

15 45 C.F.R. § 164.402.

16 Section 3 of Mass. Gen. Laws ch. 93H states that breach notices “shall not include the nature of the breach.”

17 Florida, see FLA. STAT. § 817.5681(1)(a); Ohio, see OHIO REV. CODE ANN. § 1349.12(B)(2); and Wisconsin, see WIS. STAT. § 134.98(3), have such requirements.

Chair's Corner

Gerald “Jud” E. DeLoss, Esquire

Krieg DeVault LLP

Chicago, IL

What hasn't the Health Information Technology Practice Group (HIT PG) done for you lately? That is the question I am asking you, loyal HIT PG members. What is HIT *not* providing that you *need*? What is the HIT PG *not* providing that you *want*?

We have seen enormous changes in the ways in which information is being disseminated to the public: the web, Real Simple Syndication, blogs, Twitter, Facebook, LinkedIn, YouTube, etc. At the same time, the traditional newspaper model is said to be almost extinct. Clearly, the way we as health lawyers gather our information has also changed. The HIT PG currently utilizes the Discussion List, *HIT News*, webinars, and Member Briefings. We want to remain a constant source of information for you. Would you prefer a different format than the traditional newsletters? What new vehicles, models, or technology do you find the most convenient? These questions and others like them will guide the HIT PG leadership as it charts out the rest of the year.

To get this process started, here are some current items being discussed and implemented. First, the Electronic Health Records (EHR) Affinity Group has been created to address the legal issues related to the adoption of EHRs. We felt an affinity group was a more streamlined method for gathering collective knowledge and preparing deliverables to our membership. Second, the HIT PG is in the early stages of planning an in-person program, perhaps similar to the Masters Program held in the past, for HIT PG members to focus exclusively on HIT issues. Our current structure has no stand-alone program or event. Third, the HIT PG has placed an emphasis on guides such as the excellent HITECH Act Resource Guide, which provides more practical, concrete information, rather than theories or legal overviews. Finally, the HIT PG website is updated with all of the recent HITECH Act- and ARRA-imposed changes.

Let me know what you think—good or bad—via email, Tweet, IM, or a good, old-fashioned phone call (see page 5 for contact information).

Jud