The views are those of the authors and do not represent the position of the Association. Health Lawyers is a non-partisan educational organization that does not take positions on public policy issues and instead provides a forum for an informed exchange of views. Health Lawyers invites those with opposing views on the Feature to submit letters or articles, which will be reviewed, published and edited on a space available basis. Letters to the Editor should be no longer than 250 words in length. If those seeking to respond would like to do so in the form of an article, he or she may submit it for consideration to editorial@healthlawyers.org, and the proposed article will be considered in the ordinary editorial process.
Stolen laptops. Lost packages. Missing data tapes. Media reports of information security breaches inside and outside the health industry are becoming an every day event. Hot on the heels of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), more and more states are enacting laws that require varying types of information security breach notification. Particularly for large organizations, such as multi-state health plans, keeping pace with these laws is an increasing challenge.

The following article is designed to help bring readers up to speed on some of the key elements and unique variations across state notification laws. It will also address how these laws interact with some of the existing obligations under HIPAA, as well as federal healthcare program requirements. The article concludes with a discussion of prevention and mitigation strategies that an organization can implement now to help minimize potential enforcement threats.

Setting the Stage

The size and expense of the information security breach problem in the United States today is staggering. In a May 2007 survey, 85% of companies surveyed reported suffering within the previous 24 months a data breach involving the loss or theft of customer, consumer, or employee data. In 81% of these instances notification was required, and 57% of respondents reported having no incident response plan in place. An earlier survey found the cost of information security breaches to average $99 per compromised data record.

As a recent example, The TJX Companies Inc. announced in September 2007 that the settlement of consolidated class actions resulting from the breach of at least 46 million customer records would cost the company in excess of $100 million. This total does not include, of course, expenses related to the enforcement of the breach by state and federal authorities, nor the costs of any changes to systems and business processes designed to prevent similar breaches in the future.

The cost and expense of information security breaches has not been limited to the private sector. In May 2006, a laptop containing information on 26.5 million veterans was stolen from the home of a Veterans Administration employee. Although the laptop was later recovered by law enforcement, who determined that no sensitive personal information had been compromised, the fallout from the incident was significant.

As but one example, the U.S. Government Accountability Office (GAO) began to issue a series of reports in which security breach issues were addressed. One such report highlighted the experiences of contractors participating in various federal healthcare programs. In particular, the report noted that between 2004-2005, 47% of Medicare Advantage contractors, 42% of Medicare fee-for-service contractors, and 38% of TRICARE contractors reported experiencing a privacy breach.

In response to the GAO report, the Centers for Medicare and Medicaid Services (CMS) highlighted a June 26, 2006 memo in which it informed plans participating in Medicare Advantage and Part D that they must notify CMS of any security breaches involving personal health information. CMS also indicated that the Office of Inspector General (OIG) for the U.S. Department of Health and Human Services (HHS) would...
be assisting CMS “in investigating health plan capability in this area,” including “assessing whether contracted health plans have adequate security controls in place for handling personal health information.”  

**Overview of State Laws**

As 2007 drew to a close, at least 39 states and the District of Columbia have passed some form of information security breach notification law. Generally speaking, these laws tend to follow the format originally established in California’s security breach notification law, which was enacted in 2003. The laws tend to require some form of notification in the event the security of a computer system is breached such that unencrypted “personal information” (or equivalent term) maintained in the electronic data was, or is reasonably believed to have been, acquired by an unauthorized person. As discussed below, how “personal information” or equivalent term is defined can vary, but it typically encompasses a person’s first name or initial and last name, plus one of the following types of information pertaining to the person: Social Security number; driver’s license or other state identification number; or an account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to the person’s financial account.

For healthcare organizations familiar with HIPAA, it is important to keep in mind that the purpose of these laws is generally to prevent identity theft, not necessarily simply to protect the privacy of information. As a result, there may be information that falls under HIPAA that does not necessarily meet the definition of “personal information,” depending on the jurisdiction at issue.

**As 2007 drew to a close, at least 39 states and the District of Columbia have passed some form of information security breach notification law.**

Despite some common themes among the state laws, what can make them tricky from a compliance standpoint—particularly for organizations with customers or operations in multiple states—is the subtle, and sometimes dramatic, variation that can occur from state-to-state.

“Personal information,” for example, is defined in Arkansas to include a person’s name in combination with his or her “medical information,” arguably stretching the definition beyond the purpose for which these laws have been established (i.e., to prevent identification theft). In North Dakota, “personal information” includes a person’s name in combination with “[a]n identification number assigned to the individual by the individual’s employer.” From a health plan perspective, this begs the question whether a number assigned to an employee participating in an employer-sponsored health plan meets North Dakota’s statutory definition of “personal information,” even if it is not a Social Security number. Among other variations, states differ in defining the threshold for when notification is necessary (e.g., where security is “materially compromised,” or where there is a “significant risk” of harm), time limits for notification (e.g., 45 days), whether notification must also be made to a state agency, whether the law applies to both electronic and paper records, the content of the notice, and the extent to which exemptions may apply.

Many state notification laws also incorporate some form of “pre-breach” requirement. For health entities well versed in the security requirements under HIPAA, many of these state requirements will seem familiar. For example, such laws may require reasonable and adequate security procedures, contractual safeguards for transfers, and effective and timely document destruction methods and policies. As under HIPAA, encryption is generally not mandatory under these laws; however, this may be required down the road as the technology becomes less expensive and easier to implement.

**Enforcement Threats**

In significant contrast to HIPAA’s rather passive enforcement history, state security breach notification laws have been a catalyst for significant enforcement activity. State attorneys general, in particular, have been actively investigating companies that have suffered breaches. The TJX Companies Inc., for example, is facing a joint investigation by 37 state attorneys general as a result of the recent breach of 46.5 million customer records. Those found to have violated a notification law may face civil penalties, injunctive relief, and costs and attorneys’ fees, not to mention the cost of responding to the investigation. Some state notification laws provide a private right of action, if individuals suffer injury or damage from a violation of the law. In other instances, breach victims have sued on other statutory or common law theories.
such as unfair business practices, fraud, negligence, and negligent misrepresentation. To date, however, most of these private lawsuits have not resulted in plaintiff victories. For example, in an August 2007 decision, the U.S. Court of Appeals for the Seventh Circuit affirmed dismissal of a putative class action that requested compensation for credit monitoring services resulting from an apparent breach. In other words, the plaintiffs sought to recover the costs associated with monitoring their accounts in anticipation of theft, rather than damages they had actually suffered, such as monetary loss as a result of identity theft. In support of its conclusion, the court noted, “a series of cases has rejected information security claims on their merits. Most have concluded that the plaintiffs have not been injured in a manner the governing substantive law will recognize.”

In addition to state enforcement of notification laws, it is also worth noting that failure to advise individuals of a breach may result in inquiry from the Federal Trade Commission (FTC). However, once a company is under scrutiny by the FTC for its failure to provide notice, an in-depth review of all of its privacy and security practices usually ensues. The FTC has become increasingly active in enforcement of cases involving potential identity theft, and settlements with companies such as DSW, ChoicePoint and oversight by the FTC. As a result, these documents establish useful benchmarks for determining the adequacy of particular security practices.

Federal Legislation?
For the past several years, a myriad of bills have been introduced in Congress designed to establish a federal standard for information security breach notification. To date, none have successfully made it through the legislative process. One of the key issues that has emerged is whether a federal law will preempt the 39 state laws already on the books. While many companies with operations in more than one state may applaud the idea of a single standard, it has been increasingly difficult to convince Senators and Representatives that they should vote in favor of a bill that, possibly, may cripple unique provisions or heightened standards implemented in their home states. A related issue is deciding which agency should enforce a federal notification law, and whether such enforcement authority would be as effective as current efforts by state attorneys general.

Prevention & Mitigation Strategies
Unless and until a preemptive federal law is passed, health insurers

<table>
<thead>
<tr>
<th>HMOs and Health Plans Practice Group Leadership</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kevin D. Gordon, Chair Crowe &amp; Dunlevy PC Oklahoma City, OK <a href="mailto:gordonk@crowedunlevy.com">gordonk@crowedunlevy.com</a></td>
</tr>
<tr>
<td>Todd M. Ebersole, Vice Chair – Educational Programs Prescription Solutions, a United Health Group Company Irvine, CA <a href="mailto:todd.ebersole@phs.com">todd.ebersole@phs.com</a></td>
</tr>
<tr>
<td>Lisa A. Hathaway, Vice Chair – Membership Blue Cross Blue Shield of Florida Jacksonville, FL <a href="mailto:Lisa.Hathaway@bcbsfl.com">Lisa.Hathaway@bcbsfl.com</a></td>
</tr>
<tr>
<td>Stuart I. Silverman, Vice Chair – Publications Office of Inspector General for the District of Columbia Government Bethesda, MD <a href="mailto:stuart.silverman@dc.gov">stuart.silverman@dc.gov</a></td>
</tr>
<tr>
<td>Dorthula H. Powell-Woodson, Vice Chair – Research Wiley Rein LLP Washington, DC <a href="mailto:dpowell-woodson@wileyrein.com">dpowell-woodson@wileyrein.com</a></td>
</tr>
<tr>
<td>Alan D. Bloom, Listserve Care1st Health Plan Monterey Park, CA <a href="mailto:ABloom@care1st.com">ABloom@care1st.com</a></td>
</tr>
</tbody>
</table>

Thanks go to the Practice Group for sponsoring this feature.
and others must do what they can not only to mitigate the harm resulting from a breach, but also to prevent such breaches from occurring in the first place. The following are some strategies that organizations can implement to help accomplish this goal.

As a starting point, an organization should inventory the “personal information” in its possession. This inventory should not simply be limited to what would qualify as “protected health information” under HIPAA, but also should include the personal information of employees as well.

Once this inventory has been completed, the organization should assess its vulnerability to a breach. Interestingly, a June 2007 survey of information technology (IT) practitioners found that 42% of respondents believed their organizations were doing an inadequate job of securing confidential information, and 68% believed that their organization had too much personally identifiable information scattered throughout their organizations’ systems. If this is the case, then a starting point for any organization’s assessment should be a conversation with the organization’s IT personnel regarding any concerns they may have with regard to existing system safeguards.

Next, an organization should benchmark its current security initiatives against what is required under state law and related sources, such as FTC guidance. Importantly, benchmarks against state laws should take into account not only the jurisdictions in which the organization has operations, but also the jurisdictions in which it does business and in which health plan members or other customers reside. Typically, state security breach notification laws are triggered when personal information regarding a state resident is breached.

Perhaps the most significant step an organization can take to reduce potential liability under state security breach notification laws is to minimize the amount of “personal information” (as defined by relevant statute(s)) that it maintains. For example, an organization can move away from using Social Security numbers as identification numbers. Alternatively, use of encryption technology often can render otherwise “personal information” outside the scope of a state notification law.

Additional recommended preventative measures are consistent with what many healthcare organizations are already doing for purposes of HIPAA compliance. Such measures would include the following: limiting access to personal information; utilizing adequate administrative, technical, and physical security safeguards; requiring adequate security of third parties through contract (e.g., by updating existing HIPAA business associate agreements); use of intrusion-technology to detect breaches rapidly; and disposal of personal information in a timely and effective manner.

Of course, sometimes even the best of efforts cannot stop a security breach from occurring. As a result, organizations should also anticipate what measures will be necessary to respond to a breach effectively. A first step should be identification of an internal response team. Such team may include members of the organization’s IT, Legal, Human Resources, and Communications/Public Relations departments. Once assembled, the team should assign tasks and responsibilities. The team also should run practice drills that anticipate different breach scenarios. For example, the team should practice how the organization would react if the breach was discovered over a weekend or holiday.

The organization also should consider developing template documents likely to be used in the event of a breach. This could include one or more model notification letters that could be modified to include the facts of a particular scenario. Similarly, the organization—with assistance of legal counsel—can develop template filings for a temporary restraining order or preliminary injunction relief, in the event the organization’s trade secret or confidential business information were to be breached (e.g., executive compensation information).

Another recommended mitigation measure is to develop contacts and relationships at one or more of the credit reporting agencies (Equifax, Experian, TransUnion). Many state notification laws require notification to credit reporting agencies in circumstances where a large number of persons is impacted by the breach. In addition, although state laws do not typically require purchase of credit monitoring services for breach victims, as a practical matter, it has become common for companies to offer such complimentary services for victims, particularly where the likelihood of identity theft
resulting from the breach is high. Having an established relationship with one or more credit monitoring agencies can enable an organization to save precious time in the course of breach mitigation.

As a related matter, the response team should develop a list of contact information for any state agencies that require notification in the event of a breach. At least one state, New Jersey, actually requires notification to the state before notification is made to individual breach victims. To this end, the response team may consider developing a flow chart that it can use to follow its decision making and ensure that the necessary and appropriate notification obligations are satisfied.

Finally, an organization should implement a comprehensive employee training program. This training should include not only measures employees can take to safeguard existing personal information, but also activities employees should recognize as suspicious and that might represent the sign of an attempted breach.

**Challenges**

With nearly 80% of states having implemented some form of security breach notification law, virtually every organization that handles personal information—health plans among them—must understand the laws that may apply to their operations, and develop plans to comply with these laws. System breaches can be unnerving and stressful experiences. Significant forensic investigation and critical decisions must be executed in a very short time frame. Questions such as what information was lost, how the breach occurred, and who must be notified can be difficult to answer quickly. However, through the development of prevention and mitigation strategies, a company can greatly reduce its exposure to a significant breach event.

Robin Campbell is a member of Crowell & Moring’s Privacy & Data Protection team. She specializes in the development and implementation of global information management strategies for the handling of personal information, including employee, customer, and consumer information. She can be reached at rcampbell@crowell.com.

3 Id.
5 The TJX Companies, Inc. Agrees to Settlement of Customer Class Actions; Subject to Court Approval; Estimated Costs of Settlement Already Reflected and Disclosed, TJX Press Release (Sept. 21, 2007).
7 Id. at 29.
8 Id. at 30.
10 Cal. Civ. Code § 1798.82.
11 See, e.g., id.
12 Ark. Code § 4-110-103.
13 N.D. CENT. CODE § 51-30-01.
16 See, e.g., Cal. Civ. Code § 1798.84.
17 Piscotta v. Old National Bancorp, 499 F.3d 629 (7th Cir. 2007).
18 Id. at 639 (citations omitted).
20 Ponemon Institute LLC, What Worries IT & Compliance Practitioners Most about Privacy and Data Security? (June 1, 2007), referenced in Sharon Gaudin, IT Managers See Risk of Data Loss is Bad and Getting Worse, InformationWeek (June 18, 2007).
21 See, e.g., Fla. STAT. § 817.5681.
22 See, e.g., 815 Ill. COMP. STAT. 5/10 (limiting “personal information” to circumstances when “either the name or the data elements are not encrypted or redacted”).
23 See, e.g., Tex. BUS. & COM. CODE § 817.5681.
24 N.J. STAT. 56:8-163.12.c.(1).