The Electronic Age: Liability and Insurance Coverage

Law360, New York (January 07, 2013, 6:05 PM ET) -- HIPAA, HITECH Act and ARRA are just a few acronyms of federal statutes that serve as the cornerstone for the protection of sensitive personal health information (PHI) in the ever-expanding electronic age of health care. Health care electronic data breaches continue to raise real concerns for both patients and health care providers and institutions.

The Health Insurance Portability and Accountability Act provides for civil and criminal penalties to be imposed on persons who improperly handle or disclose individually identifiable health information. For the patient, the concerns over identity theft and disclosure of confidential medical information arise when a breach has occurred. For the health care provider, the obligation to properly safeguard the data in the first instance gives rise to a variety of economic costs once there has been a breach. The civil costs can include expenses associate with investigations, audits, notification requirements, attorney’s fees and civil fines. There is also the possibility of criminal liability.

Enacted in 2009, the Health Information Technology for Economic and Clinical Health Act (HITECH Act) sets forth the reporting obligations for an organization if it has experienced a privacy breach impacting information for more than 500 people, including notifying the affected individuals, the secretary of the U.S. Department of Health and Human Services and the media.

In 2011, the American Recovery and Investment Act of 2009 (ARRA) began providing financial incentives for the use of electronic health records. The continued movement toward using and relying on electronic records increases the frequency and costs associated with these types of breaches.

Since the enactment of the HITECH Act, the incidents and reporting of data breaches has been on the rise as evidenced by the settlements reached with the government and actions filed in state and federal courts. Given this increase, proper safeguards and policies should be instituted to protect against data breaches in the first instance.

When those fail, liability issues may be created. Understanding those liabilities and the possible risks associated with them has led to the development of insurance products that are meant to address some of the exposures and financial consequences of a data breach.

In addition to federal legislation, the majority of states have enacted legislation to protect the consumer by requiring businesses to notify both the individuals affected by the data breach as well as the applicable state or federal agency and/or media. As of Aug. 20, 2012, 46 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation involving protection of personal information. Alabama, Kentucky, New Mexico, and South Dakota have no security breach laws. (See National Conference of State Legislatures website.)
While the legislative reporting obligations may provide some relief to the consumer, the enforcement provisions are left to the individual state’s attorney general or the federal government. Under the HITECH Act, for example, a state attorney general is given the authority to bring civil actions on behalf of state residents for violations of the HIPAA privacy and security rules. The HITECH Act permits a state attorney general to obtain damages on behalf of state residents or to enjoin further violations of the HIPAA privacy and security rules.

In terms of examples of specific breach cases, in 2011, the Office for Civil Rights (OCR) reached an agreement over a HIPAA privacy complaint with General Hospital Corporation and its affiliate, Massachusetts General Physicians Organization Inc. (Mass General). This case arose arising from the loss of 192 “hard-copy” outpatient files that were left on a subway.

The agreement included a $1 million penalty for the failure to implement reasonable and appropriate safeguards to protect the privacy PHI when removed from Mass General’s premises. The agreement also involved a three-year corrective plan, training for employees and appointment of an internal monitor to conduct periodic assessments and provide reports to the HHS semi-annually.

In March 2012, the HHS entered into a $1.5 settlement with BlueCross BlueShield of Tennessee to settle health care information privacy and security violations under HIPAA. This was the first case involving a civil monetary penalty issued by the OCR for a covered entity’s violation of the HIPAA privacy rule based on the HITECH Act amendments.

BlueCross reportedly incurred more than $17 million in direct expenses related to its investigation and remediation of the incident. That incident involved a failure to implement appropriate administrative safeguards to protect information by storing PHI on unencrypted computer hard drives. Under its settlement agreement, BlueCross Blue Shield also agreed to undertake a review of its policies and implement training of its employees for HIPAA compliance.

Other case examples and resolution agreements reached in 2012 include: a $1.5 million settlement by a Massachusetts provider in September; a $1.7 million by the Alaska Department of Health and Social Services and a $100,000 settlement in April with a Phoenix cardiac surgery group (see HHS website).

Given the privacy concerns of individuals over the disclosure of confidential medical information, it is not unexpected that individuals continue to seek redress in the courts, notwithstanding state and federal enforcement actions. Several courts have found that Congress did not intend for private enforcement of HIPAA’s requirements for the confidentiality of a patient’s medical records and have refused to allow private rights of actions for alleged HIPAA violations under a variety of circumstances.[1]

The lack of a private right of action under HIPAA has not curtailed civil litigation by individuals or as a member of a class action. Class actions have been brought asserting negligence claims and unfair trade practices claims under state statutes after unencrypted patient records containing personal, medical and financial information were stolen. In Paul v. Providence Health System, 237 Or.App.584 (2010) the Oregon Court of Appeals held that the mere theft of such information did not constitute a present physical injury. The economic cost of ongoing credit monitoring was an insufficient injury on which to base a negligent claim.

Furthermore, the court found that the health system did not owe the patients a special duty beyond the general duty of reasonable care to safeguard the records from theft. In so holding, the court rejected the plaintiffs’ arguments that the federal and state law
protecting confidentiality of health information created a heightened duty.

Claims for unfair trade practices failed for similar reasons under the Paul decision. The out-of-pocket expenses to monitor credit and prevent potential identity theft did not amount to "ascertainable loss of money or property" under the Oregon statute.

In Slaughter v. Aon Consulting Inc. (Superior Ct. Del. 2012), the Delaware Superior Court cited Paul and other cases when it granted Aon’s motion to dismiss a class action brought by retirees. The retirees had alleged that Aon negligently breached its contract to protect sensitive information in violation of Delaware law.

In doing so, however, the court expressed that it was “troubled by” the string of cases upholding dismissals for these types of actions. The court suggested that this might be an issue for the legislature to address.

Contrary to the decisions in Paul and Slaughter, however, 2012 also resulted in decisions in which the courts found in favor of individuals who were seeking to bring class actions under a variety of legal theories for alleged identity theft incidents. In Worix v. Medassets, 869 F. Supp. 2d. 893 (N.D. Ill. 2012) and Resnick v. Avmed Inc., 693 F.3d 1317 (11th Cir. 2012), the courts recognized certain causes of actions for plaintiffs who sought relief against a company that handled personal and confidential information for hospitals and a plan operator, respectively.

In both cases, the courts granted in part, and denied in part, motions to dismiss. These cases may represent the beginning of a trend in which courts find that individuals have stated causes of action over data breach incidents sufficient to withstand motions.

In Worix, a patient brought a putative class action in Illinois state court against a company that handled personal and confidential information for hospitals. He alleged violations of the Stored Communications Act (SCA), Illinois Consumer Fraud Act (ICFA) and Illinois common law. Following removal to federal court, the district court initially dismissed the complaint. Upon reconsideration, the district court held that the company’s alleged failure to take reasonable steps to safeguard the patient’s personal data did not violate SCA. Similarly, the court held that the company had no duty under the Illinois Personal Information Protection Act (PIPA) or HIPAA to provide patients with prompt notice that their personal and/or medical data had been compromised.

It also found that the company did not have a duty to patients to protect information from disclosure. Similarly, the court held that the company had no duty under the Illinois Personal Information Protection Act (PIPA) or HIPAA to provide patients with prompt notice that their personal and/or medical data had been compromised.

Unlike the decision in Paul referenced above, though, the district court held that the patients had stated an unfair practice claim under the ICFA and had adequately alleged compensable injury. The court concluded that the combination of damages Worix alleged — a risk of future harm, the cost of credit monitoring, emotional distress and lost wages — constitutes a sufficient allegation of compensable injury under the ICFA.

In Resnick, current or former members of health care plans brought an action against a plan operator in Florida state court. The suit contained allegations relating to identity theft incidents that occurred after unencrypted laptops containing members’ sensitive information were stolen from the plan operator’s corporate office. The issue of whether a party claiming actual identity theft resulting from a data breach has standing to bring suit was an issue of first impression for the 11th Circuit.

Plaintiffs alleged claims under Florida law for negligence, negligence per se, breach of contract, breach of implied contract, breach of implied covenant of good faith and fair dealing, breach of fiduciary duty and restitution and unjust enrichment. The matter was removed to federal court, where the district court dismissed the complaint for failure to state a claim.
On appeal, the 11th Circuit Court of Appeals held that the plaintiffs had stated claims for each of the theories listed above with the exception of the claims for negligence per se and breach of implied covenant of good faith and fair dealing. In so holding, the court noted, “in this digital age, our personal information is increasingly becoming susceptible to attack.”

According to the 11th Circuit Court of Appeals, cases brought by these alleged victims are held to the same pleading standards imposed by courts in all civil suits. The plaintiffs in Resnick pled a cognizable injury and sufficient facts to allow for a plausible inference that AvMed’s failures in securing their data resulted in their identities being stolen. They also demonstrated a sufficient nexus between the data breach and the identity theft.

With the ever-increasing exposure posed by enforcement and the viability of civil actions, those charged with protecting electronic health information need to take affirmative steps to review their compliance programs and institute the relevant training programs for their employees. In terms of risk management, an ongoing review and assessment of available insurance coverage is also warranted. Policies are available that may provide some type of coverage for breach of security claims.

Coverage may include payment of attorney’s fees incurred in representing an insured in the event of a security breach. They may also include the costs associated with notification under state statutes, card issuer regulations and credit monitoring payments if the Insured has suffered a security breach, resulting in unauthorized acquisition of computer data that compromises the security, confidentiality or integrity of person information maintained by an insured.

It should be noted that a policy may not provide costs associated with the adoption and implementation of any corporate integrity agreement, compliance program or similar provision regarding the operation of an insured’s business negotiated as part of a settlement with or by order of a government entity.

Cybersecurity insurance is another form of insurance that might be considered. These policies may cover risks associated with both first-party and third-party risks. The former being available to cover potential costs for loss of or damage to the policy-holder’s own data or lost income due to a data breach or cyber attack. Third-party coverage should be considered to cover an insured’s potential liability to individuals or governmental or regulatory entities described above.

Given the relatively new area of these types of policies, there have not been that many reported cases addressing the specific coverage issues that might arise in the event of a claim. In Retail Ventures Inc., et. al. v. National Union Fire Ins. Co., et. al, 691 F. 3d 821 (6th Cir. 2012), for example, the Sixth Circuit found coverage for a retailer’s losses from a 2005 computer hacking incident under a “blanket crime policy” and a computer fraud rider.

These losses included the expenses incurred for communicating with and handling customers’ claims, conducting a public relations campaign, litigating lawsuits and implementing an information security program. The total amount paid by the insurers was $6.8 million.

For those insurers who are underwriting these types of policies, it is imperative that a thorough underwriting review include an assessment of the insured’s privacy policies, including proper encryption and internal employee training and compliance programs. This is an area where the consequences for a data breach and/or a cyber attack will continue to be significant and costly for both the insured and its insurers.

In the event of a data breach, it will be important for the insurer to work with its insured
and its counsel to ensure a prompt investigation and response to minimize any alleged exposure and resulting damages.

--By Carol J. Gerner and Fred A. Smith, Sedgwick LLP

Carol Gerner is a special counsel and Fred Smith is a partner in the firm's Chicago office.

The opinions expressed are those of the authors and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] See, e.g. Acara v. Banks, 40 F.3d 569 (5th Circuit 2006) (HIPAA did not create a private right of action for a doctor’s alleged violation of confidentiality provisions of the act in disclosing the patient’s medical information during a deposition without her consent); Muringi v. Touro Infirmary (E.D. La. 2012) (Court dismissed plaintiff’s employment claim alleging violations of HIPAA concluding that he did not have standing to bring a private right of action under HIPAA); Padilla-Ruiz v. United States (D. Puerto Rico 2012)(No private right of action for reservist in connection with the alleged release of false medical and private information to investigators who were conducting an administrative Army investigation).

All Content © 2003-2013, Portfolio Media, Inc.