



Q&R STRATEGIST

[Volume 5 · Issue 2 · August 2009]

AON RISK SERVICES

Q&R Strategist addresses Quality and Risk issues for health care.

Potential privacy liability risks are not limited to those organizations that directly provide health care services. Any organization that touches or handles Personally Identifiable Information (PII) and/or Protected Health Information (PHI) is exposed to these risks in some form, regardless of whether or not they are subject to the Health Information Portability and Accountability Act (HIPAA).

This article is intended to give the reader an overview of some of the factors in the privacy liability equation as it pertains to the health care industry. For additional information on this issue, you may contact Aon Healthcare for a copy of a longer white paper addressing this issue. Please contact Karen_Cullinane@aon.com to request the white paper or with any questions.

Privacy Liability and the Health Care Industry

By Sarah Stephens and Shannan Fort, Aon Financial Services Group

Health Care Privacy Liability Risk Profile and Exposures

Due to the nature of operations and the use of PII/PHI in almost all facets of the organization, health care firms have more channels of exposure than those in many other industries. Some reasons for this heightened exposure are the following:

- **Many Users:** Many individuals have access to PII/PHI both within a health care organization (physicians, nurses, accounts receivable, etc.), and externally (pharmacies, insurance companies, outsourced service providers). In addition, the continued introduction of new services, such as client-facing web interfaces, opens new and evolving channels of exposure. The numerous users of PII/PHI enhance the probability of error leading to possible breaches. In fact, the human dynamic is perhaps the most critical to the exposures equation, illustrated by a recent study that concluded that three quarters of incidents involving the loss of confidential data are caused by human error¹.
- **Scope of Network Operations:** In order to facilitate availability for the numerous parties described above, network systems must be configured to allow for multiple points of access. Outsourced Information Technology (IT) entities and other service providers

may also have direct access to the health care organization's network, thus increasing exposures. Additionally, some larger health care entities have semiautonomous subsidiaries with little or no connectivity to the master network, which increases the perceived risk of the parent organization.

- **Outsourcing:** Increasingly, health care entities are utilizing outsourcing in some manner. The nature of operations outsourced may range in scale from payment processing to X-ray reviewing and lab test processing. While the cost savings of outsourcing arrangements can be attractive, these arrangements also heighten the organization's risk profile. Regardless of whether information is outsourced to a domestic or offshore firm, the contracting firm's information security protocols should be given the highest level of attention.
- **Information Technology Implementation:** Much like outsourcing, the modernization of operations and implementation of the latest technologies can result in tremendous cost savings if performed effectively. The downside, however, can be system integration problems, employee training hurdles, and unknown bugs or system glitches that can facilitate a breach of confidential information. A great deal of the focus

in health care technology surrounds the creation and implementation of Electronic Health Records (EHRs) and Personal Health Records (PHRs).

- **Other Factors:** Numerous other factors can contribute to liability scenarios, including whether a health care organization provides any services to unrelated entities. For example, many community hospitals hire larger health systems to provide services which include implementing, installing, and servicing IT platforms for clinical care and billing.

Health Care Incidents

In 2008, on average, nearly 98,000 health care-related records were breached per day² and the average cost of a health care data breach was \$282 per record³. Simple acts such as an unguarded computer, discarded patient records or an accidental post to a website can put protected health information at risk. These breaches in network security or privacy policies result in the exposure or loss of PII/PHI and can lead to costly settlements, fines, and other losses such as lost business. In fact, lost business accounted for over 69% of data breach costs in 2008.

Health care breach incidents can involve PHI and PII in any form or media, whether electronic, paper or oral. The potentially exposed information does not originate only from patients or customers or health care institutions, but rather any confidential information that the health care organization possesses, including that of its own employees.

According to the Ponemon Institute's 2008 Data Breach Survey, the average data breach, across all industries, costs \$202 per exposed record, for an average total of \$6.6 million per breach. These costs include legal fees, notification expenses, investigation expenses, identify theft mitigation measures (for example, credit monitoring and call centers) and lost business. Interestingly, the average cost of a health care data breach was almost 40% higher than the all-industry average, at \$282 per record. For specific examples of the potential severity of a breach, here are details⁴ of three of the largest publicly reported health care breaches to date:

- A laptop and external hard drive from a government health care organization containing sensitive data (name, date of birth and social security numbers) on over 26,500,000 veterans were stolen from an employee's home. After three years of litigation over this data breach, a federal judge approved a \$20,000,000 settlement.

“...THE AVERAGE COST OF A HEALTH CARE DATA BREACH WAS ALMOST 40% HIGHER THAN THE ALL-INDUSTRY AVERAGE, AT \$282 PER RECORD.”

- A university hospital's back-up tapes containing approximately 1,300,000 patients' and guarantors' health care billing records were stolen from the car of an outsourced data storage company employee. The hospital spent \$500,000 to notify those affected by the breach and offered one year of free credit monitoring to those 1,300,000 people who were affected by the breach at a likely cost of over \$3,000,000. In addition, within a month of the announcement of the breach, two patients filed proposed class action lawsuits. Though the tapes were recovered, the lawsuits were not dropped until almost six months later, causing the hospital to incur significant defense expenses.
- Media containing 365,000 medical records of a major hospital system were stolen from an employee's car. The hospital hired forensic experts to assess the scope of the breach, set up a call center; created an informational web site, and called patients whose financial information was compromised. The estimated cost of the incident response was seven to nine million dollars. The state attorney general took action against the system and the HHS OCR initiated an investigation in response to more than thirty consumer complaints. The hospital settled and agreed to pay for three years of credit monitoring and credit restoration services for affected patients, to designate an employee to coordinate information security for the hospital, to enhance its data security company, including conducting risk assessments, providing worker data security training and regularly testing the security system, to pay all claims for direct financial loss that result from the breach, and to pay \$95,000 to the state's consumer protection education fund. The system also paid a \$100,000 fine to HHS and agreed to adhere to a compliance plan under the first-ever "Resolution Agreement" executed pursuant to the HIPAA Privacy Rule.

Risk Management Strategies

- **Technology & Strategy:** It is critical that each health care organization use technology that complements its security policy; a multitude of products have been specifically designed to fit the changing needs of the health care community. Additionally, because health care is an ever-changing industry and also one that is guided by stringent regulations, the technologies employed must keep pace with the current environment.
- **Contractual Allocation of Risk:** As 30 percent of all reported breaches are attributed to external partners, consultants, outsourcers and contractors, it is critical to determine the boundaries of liability when PII/PHI is shared for business purposes. The failure to do so can result in confusion and disarray when a breach occurs. Even a standard outsourcing arrangement, like the one the U.C. San Francisco Hospital had with TranscriptionStat, can result in problems. TranscriptionStat handled the large hospital's transcription work for over twenty years until a rogue transcriptionist outsourced her work to a Pakistani sub-contractor without the approval of her employer or the hospital. The sub-contractor then threatened to post the confidential medical information unless she was paid a certain amount of money⁵. Although the debacle was resolved before the information was exposed, it highlights one of the possible liability issues health care firms face.

Appropriate contractual provisions in business associate agreements and outsourced services arrangements can mitigate the effect of these situations by clearly defining responsibility, ensuring

the proper precautions are taken when the information is out of the control of the health care organization, and limiting the liability of the health care organization in the unfortunate event of a data breach. Specifically with respect to appropriate insurance requirements for PII/PHI risks, we suggest a targeted and well defined provision along the following lines:

Errors & Omissions/Privacy Liability Insurance, in an amount not less than \$XX,000,000 per claim and annual aggregate, covering all acts, errors, omissions, negligence and network risks (including coverage for unauthorized access, failure of security, breach of privacy perils, as well as notification costs and regulatory defense) in the performance of services for <name> or on behalf of <name> hereunder. Such insurance shall be maintained in force at all times during the term of the agreement and for a period of five years thereafter for services completed during the term of the agreement. <Insured> shall be given at least 30 days notice of the cancellation or expiration of the aforementioned insurance for any reason.

Because the elements of exposure are completely dependent on each organization's unique operations and policies, a generic insurance requirement should be avoided if possible. Many business-to-business contracts still contain very basic requirements that may only minimally address a liability component. It is important that coverage provides for costs that result from a breach that are driven by notification, mitigation and regulatory investigations/penalties.

Risk Transfer Options — Coverage under Existing Policies

- **General Liability and Property Policies:** All insureds should review their traditional insurance policies to determine the exact scope of coverage for data breaches. Changes in 2004 to the Insurance Service Organization ("ISO") forms, as well as some insurance litigation, have limited the coverage available under traditional general liability and property forms; exclusions are becoming more common as general liability carriers offer standalone network security and privacy policies. Additionally, an increasing number of Health Care Risk Retention Groups are formalizing exclusions for all "Cyber Risks."

- **Health Care Professional Liability:** In the health care space, professional liability policies are intended to cover third-party damages and personal/bodily injury from errors, omissions or negligent acts in the course of medical care and related administrative services. It is possible to endorse security and privacy coverage on to some health care professional liability policies. Most health care entities, however, have elected to keep their security and privacy programs separate to avoid a shared limit and retention and to take full advantage of the marketplace, since only a limited number of carriers will combine the programs.
- **Other Insurance Policies:** Depending on the facts of the data breach and the particular wording of the policies, some coverage could exist in various

other policies, including commercial crime policies, employment-related practices policies, data processing policies, computer fraud policies, advertising, or kidnap and ransom (K&R) policies. For instance, if a hacker claims that confidential information will be distributed on the internet unless the insured pays some type of extortion fee, some K&R policies may provide defense and indemnity coverage. In general, however, such policies were not intended to cover privacy/data breaches and there are significant coverage gaps in each.

- **Security and Privacy Liability:** Security and privacy liability insurance (also called cyber liability or network risk) is designed to respond to third-party liability and related defense costs, as well as some of the insured's costs following a breach of the security and/or privacy of data. The available coverage parts include the following:

First Party Coverage Part	Covers:
Information asset	Damage to or theft of the insured's information assets from its computer system.
Business interruption	Lost income suffered as the result of a system outage or extended downtime due to failure of security.
Cyber extortion	Extortion threats to commit an intentional computer attack against you.
Crisis management/identity theft expenses	Various costs, such as notification, credit monitoring and public relations, resulting from a security/privacy breach.
Third Party Coverage Part	Covers:
Professional services coverage	Acts, errors, or omissions in the course of providing professional services other than medical services.
Content/media liability	Personal and advertising injury and some intellectual property infringement arising out of media content created, produced or disseminated by the insured.
Network security liability	Breaches in network security or unauthorized access events.
Privacy liability	Wrongful disclosure of confidential information.

Health care entities considering this coverage should note that the information asset and business interruption coverage parts have not been especially relevant to the health care industry, due in part to the slow adoption of advanced information technology in the industry. There are exceptions, however, and one example is an entity whose primary revenue stream is from network/internet activities, such as online pharmacies. Additionally, there have been few first-party claims paid by any insurer and significant hurdles to coverage exist, such as waiting periods of 6-18 hours before coverage applies and difficulty in valuing intangible assets and business interruption costs.

Underwriting Process

The first step in the underwriting process is the completion of an application and/or self-assessment. It is important that the risk management team engage the appropriate information security and privacy personnel in the application process to provide complete and accurate information. The assessment and application process also provides an opportunity to critically examine an entity's information risk management strategies.

In conjunction with the base application, a potential insured should be prepared to provide the following:

- Copies of privacy policies
- Standard contracts and business associate agreements
- Results of any external or internal audits or assessments that illustrate the information security posture—examples include SAS 70, PCI, or ISO 27799/27001.
- Details of any security breach incidents and the response to them, including any new protocols put in place to prevent similar incidents.
- Financial information
- Patient statistics
- Payment processing
- Outsourced services

In addition to an analysis of the standard application materials, underwriters will ask targeted questions in response to the current environment and the latest breach incidents. Recent concerns include independent contractors and business associates, data encryption protocols and wireless access security.

Aon recommends that, as part of a comprehensive risk management strategy, health care entities work with experienced brokers who are experts in security and privacy coverage and the corresponding legal issues and who have a thorough understanding of the evolving dynamics of both health care and the insurance marketplace. The underwriting process must be skillfully managed and the complexity of coverage demands innovation and expertise. Those companies who successfully utilize these resources in their risk management process will realize the benefits of this enhanced coverage.

Definitions:

Breach Notification Framework: Until recently, there was no federal breach disclosure mandate, but health care entities are subject to the framework of 45+ state breach notification statutes. While some states allow exceptions for breaches involving encrypted data, most require swift public disclosure of any potential breach of personally identifiable information. Some of these statutes have provisions that exempt entities subject to HIPAA, but only to the extent that the offending entity already has security, privacy, and notification policies in place. If a HIPAA entity does not have such policies, then the appropriate statute is applicable in the event of a breach of personal health care information.

Certification Commission for Healthcare Information Technology (CCHIT): This organization was developed jointly by HHS and several leading industry groups. CCHIT certifies technology vendors and their products for effective use in the health care community and is also a great resource for those responsible for HIP procurement.

Electronic Health Record (EHR): An electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be created, managed, and consulted by authorized clinicians and staff across more than one health care organization.

Fair and Accurate Credit Transactions Act (FACTA): FACTA added sections to the Fair Credit Reporting Act (FCRA) intended to help protect consumers from identity theft. It also contains a “red flag” provision that requires any entity considered a creditor or financial institution with a “covered account” to adopt a written plan to detect red flag events related to consumer accounts that could indicate identify theft by August 1, 2009. (This deadline has been postponed to November 1, 2009.⁶) The FTC’s guidance to health care providers indicates that many are likely to qualify as creditors because they accept payment for services after the fact, but each entity must determine whether or not they are required to be compliant. One recent study⁷ by KPMG suggests that many health care entities will need to become compliant and provides a number of suggestions to start the internal discussion. FACTA does not mandate specific data security or privacy standards but the red flag compliance process should dovetail with an organization’s data breach response plan and provide a valuable opportunity to examine breach

readiness and mitigation activities.

Health Information Portability and Accountability Act (HIPAA): Passed in 1996, HIPAA was one of the first statutes that specifically concerned any form of confidential or personal information. The HIPAA framework contains a Security Rule (passed in 2003) that loosely dictates protocols for the protection of electronic PHI, and a Privacy Rule (passed in 2002) that outlines and limits the way PHI in any form can be disclosed, as well as provisions for fines or penalties in the event of non-compliance with either rule.

In July of 2008, the Department of Health and Human Services (HHS) levied the first HIPAA fine, or rather, “resolution amount,” against Providence Health and Services for \$100,000⁸. The Providence fine was the result of a lengthy investigation into a 2005 breach involving the theft of backup tapes from an employee’s car. HHS, in conjunction with the Federal Trade Commission (FTC), levied its second fine in 2009—at the significantly larger amount of \$2,250,000—against CVS/Caremark after an investigation into improper disposal of patient information.

Health Information Technology for Economic and Clinical Health Act (HITECH Act): Included as part of the American Recovery and Reinvestment Act of 2009 (ARRA), HITECH was intended to stimulate the adoption of electronic health records, accelerate the development of a nationwide health information exchange, and strengthen the privacy and security of PHI. There has been a great deal of analysis and speculation about how this bill will affect covered entities and business associates, and as further clarification is issued by HHS, the complete picture will become more clear. HITECH has expanded the reach of HIPAA in several important ways that may affect security and privacy liability buying decisions and coverage:

- “Business associates,” and not just “covered entities” (both defined by HIPAA), are now subject to the Privacy Rule and the Security Rule.
- Civil and criminal penalties under HIPAA are now applicable to business associates.
- The first federal Breach Disclosure Law has been created, and it will apply to any breach or unsecured PHI and require compliance by covered entities and business associates, as well as vendors of EHR and PHR software.

Office of the National Coordinator for Health Information Technology (ONCHIT): This group is dedicated to the advancement and development of health care industry IT. The creation of ONCHIT also triggered an explosion of government committees and industry alliances that have produced volumes of guidance on EHR standards, which focus on functionality, availability, interoperability, and security.

Personal Health Record (PHR) (Source: HHS Report on Key HIT Terms, April 2008): An electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be drawn from multiple sources while being managed, shared, and controlled by the individual.

Plastic Card Security Act: Minnesota recently amended its data breach notification law to hold entities suffering a breach, as opposed to the issuing banks, responsible for the costs of re-issuing credit cards in the event of a data breach. The law, which was passed in the wake of the TJX security breach, can certainly pertain to health care organizations as it applies to any entity accepting credit cards, debit cards, or other stored value cards. The statute requires companies to reimburse card-issuing financial institutions for the “costs of reasonable actions” to both protect its cardholders’ information and to provide post-breach services to its cardholders. More specifically, reimbursement covers costs related to providing cardholders with notification of the breach, cancellation and reissuance of cards, closing or

reopening of accounts, stop payments and cardholder refunds for unauthorized transactions charged to their accounts. A financial institution may also bring an action to recover for the costs of damages it pays to cardholders resulting from a breach⁹. This law is specific to the state of Minnesota, but California, Connecticut, Illinois, Massachusetts and Texas have all attempted to pass similar laws. None have succeeded at this time.

Protected Health Information (PHI) (Source: HIPAA): Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

- 1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- 2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
 - i) That identifies the individual; or
 - ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Personally Identifiable Information (PII): There is no one definitive statutory definition of PII, though each insurance carrier may define the term in a slightly different way. Generally, it means any information that identifies an individual, such as name, address, telephone number, or social security number.

Footnotes:

¹ “Human error causes most data loss,” http://www.pcworld.com/article/129736/human_error_causes_most_data_loss_study_says.html

² Identify Theft Resource Center, “2008 Data Breach stats,” http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Report_2008_final_1.pdf

³ Ponemon Institute, LLC. “2008 Annual Study: Cost of a Data Breach,” February 2008.

⁴ Details of breaches compiled from news sources as well as information supplied by Hiscox.

⁵ “Protecting PHI and Responding to Data Thefts,” Davis Wright Tremaine LLP, Randy Gainer and John McCrory. www.wsha.org/files/64/Data-loss.ppt

⁶ FTC’s press release extended the compliance deadline: <http://www.ftc.gov/opa/2009/07/redflagrule.shtm> FTC’s Red Flag Rule website for businesses: <http://www.ftc.gov/bcp/edu/microsites/redflagrule/more-about-red-flags.shtm>

⁷ KPMG LLP and Katten Muchin Rosenman LLP “Business Considerations for Health Care Organizations Under FACTA: Identify Theft Prevention Programs and Address Discrepancy Resolution” March 3, 2009.

⁸ “Feds finally put teeth into HIPAA enforcement,” Computerworld, September 8, 2008. http://www.computerworld.com/s/article/325376/Feds_finally_put_teeth_into_HIPAA_enforcement

⁹ “In response to TJX data breach, one state enacts legislation imposing new security and liability obligations” Proskauer Rose LLP Privacy Law Blog. May 29, 2007. <http://privacylaw.proskauer.com/2007/05/articles/security-breach-notification-1/in-response-to-tjx-data-breach-one-state-enacts-legislation-imposing-new-security-and-liability-obligations-similar-bills-pending-in-five-other-states/>

Authors:



Sarah Stephens, AVP, Aon Risk Services, Financial Services Group

Sarah, who has over seven years of insurance industry experience, is responsible for E&O broking for a number of accounts in the healthcare, retail, technology, and financial services sectors. Sarah has an Associate in Risk Management and a B.A., with distinction, from Duke University.



Shannan Fort, Associate Broker, Aon Risk Services, Financial Services Group

Shannan focuses on security/privacy liability and technology liability for risk management clients across various industries including health care and retail. Shannan came to the FSG group after participating in Aon's Early Career Development program. Shannan has an Associate in Risk Management and a B.A., Magna Cum Laude, Howard University.

Do you know anyone who would like to be added to our mailing list?

Please email diane_salmonson@aon.com
with names, titles, companies, addresses and emails.

From the editor

Q&R Strategist is published by Aon Healthcare for electronic distribution.

Q&R Strategist encourages contributions of articles and letters on all issues pertaining to the healthcare industry. Submissions, as well as suggestions for future articles, should be sent to:

Karen Cullinane, CPCU, Director of Communications, Aon Healthcare Editor, *Q&R Strategist*

f: +1.312.381.6742 | e: karen_cullinane@aon.com

Aon Healthcare · 200 E. Randolph St.
Chicago, IL 60601 · www.aon.com/healthcare

This document is a summary review that is intended to provide information on recent developments in the health care and long-term care industry. It does not purport to be comprehensive or to offer legal or professional advice and should not be relied on as such. Aon does not warrant the accuracy of the information in the document and does not assume liability for any losses allegedly attributable to such information. As legal advice must be tailored to the specific circumstances of each case, and laws are constantly changing, nothing provided herein should be used as a substitute for the advice of competent counsel.