Network Security & Privacy
Risks in the Health Care Industry

May 2012

Aon Broking - Professional Risk Solutions

© 2012 – Aon plc

Brief Description: Conditions are ripe for health care organizations to fall prey to cyber risk. Many individuals have access to PHI and PII, both inside and outside any given health care organization. Networks and systems must be configured so that these parties can access information with speed and accuracy, while minimizing the risk of this information being compromised. The desires for enhanced efficiency and improvements in patient care (as well as HITECH incentives) have led to an explosion in the adoption of advanced health information technology. The convenience and promise of mobile and tablet computing in a clinical setting have also led to a proliferation of new, potentially less secure methods of accessing and sharing this information. Finally, due in part to budgetary pressures, health care entities are relying on outsourced service providers, ranging in scale from payment processing to lab test processing. Lax procedures by a vendor can lead to catastrophic damage to a covered entity. While insurance products professing to address these risks have been around for years, they have recently become increasingly responsive to real claim situations, and proactive health care entities have made a cyber or network security and privacy liability program a standard purchase. It is critical to work with a broker specializing in this coverage, as policy forms and insurer appetites are incredibly dynamic, just like the risks themselves.
Introduction

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 Security and Privacy Rules in the Health Insurance Portability and Accountability Act (HIPAA). There is a long list of potentially affected organizations: patient care organizations (providers), insurance companies (payors), third party administrators, technology firms creating software and hardware for the health care industry, pharmacy benefit managers, outsourced network service providers, data storage firms, Health Information Exchanges, etc.

This paper is intended to give the reader a concise view of the privacy risk landscape for the health care industry. We begin with the unique and rapidly evolving risk profile, we then summarize the regulatory and enforcement environment, provide examples of some high-profile actual incidents, and offer risk management solutions, and finally, discuss the risk transfer marketplace.

Key Terms

Protected Health Information (PHI)

*as defined by HIPAA*

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:
- Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- 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
  - That identifies the individual; or
  - 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 single, definitive statutory definition of PII. Various laws and various insurance carriers may each define the term in a slightly different way. Generally, it means any non-public personal information from which an individual can be reliably and uniquely identified as an individual, such as name in combination with address, telephone number, or social security number.
Risk Profile & Exposure Channels

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, including:

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). Additionally, the continued introduction of new services, such as sizeable client facing web interfaces, opens new and evolving channels of exposure. These numerous users of PII/PHI heighten the probability of error leading to a breach. The human dynamic is critical to the exposure equation, as illustrated by a recent study that concluded that 40% of all major PHI breaches in 2011 were 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.

Business Associates

HIPAA defines third parties with access to the PHI collected by health plans, health care clearinghouses, and certain health care providers (i.e. Covered Entities) as Business Associates. These Business Associates may perform a variety of functions for or on behalf of a Covered Entity, and they are becoming increasingly prevalent. The nature of services or outsourced operations may range in scale from payment processing, to utilization review, to lab test processing. The cost savings of outsourcing arrangements can be very attractive, but these arrangements also change the organization’s risk profile because of the increase in number of users, additional access and transfer points, loss of control, and potential inconsistencies in network security and privacy protocols.

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).

These efforts began in 2004 when a presidential mandate created the Office of the National Coordinator for Health Information Technology (ONC), a group dedicated to the advancement and development of
Health care industry IT. The creation of ONC 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. The original focus of Health IT initiatives was national interoperability, but information security and privacy have become top priorities for entities wishing to avoid the increasing probability of audits and fines. Every entity subject to HIPAA regulation should be keenly aware of compliance with the Security Rule (HIPAA established standards and implementation specifics that organizations must meet in order to become compliant) and must work to make sure the conversion to EHRs is accomplished with proper security protocols in place. Health IT meaningful use incentives in the Health Information Technology for Economic and Clinical Health Act (HITECH Act, discussed further below) have sped the adoption of EHR and e-prescribing systems.

Accountable Care Organizations and Health Information Exchanges

With the advent of Accountable Care Organizations (ACOs), experts anticipate that Electronic Health Information Exchanges (HIEs) will become critical to enhancing patient outcomes and care. Increased reliance on electronic information sharing and technology support tools will be as critically important to ACOs deriving value from government incentives, as well as delivering better patient outcomes. As ACOs seek to rely on evidence-based medicine, they will need to develop and utilize more electronic information repositories. Additionally, as they engage patients, they may reach out and create new forms of social media discussion with individual patients, as well as rely on electronic and mobile communication at new levels. For efficiency purposes, reporting on quality and cost will certainly need to be automated through electronic reporting mechanisms. Finally, coordination of care will lean on technologies beyond electronic health records and electronic health information exchanges, such as remote patient monitoring systems and web-based patient-provider interaction. In order to maintain patient trust and safety, as well as to maintain compliance with applicable state and federal law, the privacy and security of new technologies must be front and center for every ACO.

Coordination of information and systems will be a challenge in an ACO context as there are likely to be several distinct providers, payors, technology service providers, and potentially one or more health information exchanges sharing data. Each of these stakeholders may have its own Information Security personnel and philosophy, and beyond ensuring that the electronic systems are interoperable, those departments must work together to ensure that they are also sufficiently private and secure. State and federal consumer reporting requirements in the event of a breach may also be complicated due to overlapping business associate agreements requiring notification to affected consumers, applicable covered entities, regulatory agencies, or all three. It is critical for ACOs to ensure that contractual arrangements between unrelated parties specifically address who will take responsibility and bear the cost of notification and consumer communication in the event of a breach of confidential information.

Miscellaneous

Numerous other factors can also 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. The larger health system may do the training, the sales, the onsite installation, or miscellaneous functions, thus increasing its liability exposure. Additionally, if the services provided include the use or handling of the PII/PHI of the client, the service provider is likely to be held
responsible for any breaches. The smaller entity on the receiving end of such services should ensure that contractual allocations of liability and insurance provisions are drafted to provide maximum protection.

Major Regulatory Concerns

The protection of PII in general is currently governed by a patchwork of state and federal laws that target different exposures and different entities. Some of these statutes include HIPAA, Gramm-Leach Bliley Act (GLBA), Fair Credit Reporting Act, Sarbanes-Oxley Act (SOX), Privacy Act of 1974, and others. There are a multitude of regulations in place, but those most applicable to the health care industry in the United States can be separated into federal and state regulation. While we do not outline the international privacy regulatory landscape in this paper, it is important for any U.S. based health care entity treating international patients or doing business outside the U.S. to be cognizant that a variety of a privacy laws exist outside the U.S.

U.S. Federal Laws

Health Insurance Portability and Accountability Act (HIPAA)

Passed in 1996, HIPAA was one of the first statutes that specifically addressed any form of confidential or personal information. The HIPAA framework contains both a Privacy Rule (passed in 2002) that outlines and limits the way PHI in any form can be disclosed, and a Security Rule (passed in 2003) that loosely dictates protocols for the protection of electronic PHI, and, as well as provisions for fines or penalties in the event of non-compliance with either rule. Organizations violating this regulation went without penalty for years, but about the time of the passage of the HITECH Act in 2009, HIPAA finally gained teeth, and enforcement by the Office of Civil Rights (OCR) increased significantly.

HIPAA Resolved Complaints/Investigations & Fines

(Office of Civil Rights Enforcement Data)
Health Information Technology for Economic and Clinical Health Act (HITECH)

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. HITECH expanded the reach of HIPAA in several important ways that have significantly affected the way Covered Entities and Business Associates view security and privacy liability insurance buying decisions and coverage. HITECH subjected Business Associates, and not just Covered Entities, to HIPAA’s Privacy Rule and the Security Rule, both of which loosely govern the ways these entities must protect PHI. Consequently, civil and criminal penalties under HIPAA are now applicable to Business Associates as well as Covered Entities. HITECH also created the first federal breach disclosure law, and all entities suffering a breach of 500 or more individuals now must report the details and see them immortalized on the OCR website’s “wall of shame."

U.S. State Laws

State Breach Disclosure Laws

Until HITECH, there was no federal breach disclosure mandate, but many of the 49 U.S. state and territory breach notification statutes already covered PHI. 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.

State Data Protection Laws (MN, MA, NV, WA)

Minnesota 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. Washington has passed a similar law, HB 1149, which allows financial institutions to seek card reissuance costs from a breached entity. Interestingly, Washington’s law offers safe harbor if the breached entity was found to be PCI compliant in the preceding year, but does not require entities to comply with PCI. Nevada’s SB 227 modifies the state’s breach disclosure law to include a requirement for compliance with PCI, a requirement for encryption, and a very limited safe harbor from liability.

As of January 1, 2010, Massachusetts began enforcing its new, strict data protection regulations. The Massachusetts Regulation impacts almost every business that stores personal data of Massachusetts employees and residents (whether or not the company operates in Massachusetts, over the Internet or otherwise) and will require significant security and policy changes for most businesses. The Massachusetts Regulation requires, among other things, the encryption of wireless transmissions of personal information and the encryption of personal information stored on portable devices carrying personal information such as laptops, flash drives and PDAs.
Confidentiality of Medical Information Act (CMIA; CA)

California’s Confidentiality of Medical Information Act (CMIA) requires health care providers to maintain the privacy and confidentiality of medical information. CMIA allows certain disclosures without patient authorization, such as disclosures to a payor for reimbursement purposes, or disclosures ordered by a court. This law is worth specifically noting because it provides a private right of action and related statutory damages of $1,000 - $3,000 per record wrongfully disclosed. It also contains provisions for civil penalties up to $250,000. Violations of CMIA have been cited in many high profile data breach lawsuits in the past year, including those against Stanford Hospital and Sutter Health, and the statutory damage amounts have even been referenced as a benchmark in data breach cases in other states.

Health Care Privacy Incidents

Health care privacy incidents can involve PHI and PII in any form or media, whether electronic, paper or oral. According to the Ponemon Institute’s December 2011 Patient Privacy & Data Security Study, health care data breaches cost breached organizations an average of $2.2M. However, it is clear from high-profile breach incidents that a catastrophic breach with an unfavorable legal or regulatory outcome or a unique incident investigation fact pattern may cost an organization far more. Some of these incidents are further detailed below:

**Government Health Care Organization**

A laptop and external hard drive containing sensitive data (name, date of birth, and social security numbers) on over 26,500,000 veterans were stolen from an employee’s home.

**Incident response & investigation**

The FBI launched an investigation, and the equipment was subsequently anonymously returned. Several of the organization’s employees left the company due to public outrage over the breach, however it was eventually determined that no information on the devices had been improperly accessed.

**Litigation & Settlement**

After three years of litigation by the “victims” of this data breach, a federal judge approved a $20,000,000 settlement.

**Health Care Network**

In two separate incidents, the unencrypted confidential information of over 4,200,000 patients was compromised due to theft.

**Incident response**

The company set up a website and call center where affected individuals could call for additional information. Since the information did not include social security numbers or financial...
information, typical credit monitoring services were not offered. The website also assured patients that the company was accelerating efforts to deploy encryption across the organization.

**Litigation / enforcement proceedings**

The initial class action complaint was filed on the same day as the patient notifications were mailed, causing many to call it a “zero-day” lawsuit. 12 additional class action lawsuits were filed, and all such complaints were consolidated within three months. Regulatory actions are likely to follow.

**Health Insurance Plan**

Hard drives containing close to **1,000,000 member records** were stolen from an off-site facility.

**Incident response**

The company hired outside forensic experts and temporary employees to perform a manual review of backup files and assess the scope of the breach and identify the individuals affected, as well as sent written notification including an offer of credit protection services to the individuals. The company publicly disclosed that their cost for breach response exceeded **$10,000,000**.

**Litigation / enforcement proceedings**

HHS OCR initiated an investigation into the incident, and eventually levied a **$1,500,000 fine**, even though there was no evidence that any affected consumers had actually been harmed. Several state AGs have requested additional information.

**Outcome**

The company’s proactive and open communication throughout the breach response has been cited as a “model response” by multiple experts, and the fact that they were still fined could be an unwelcome harbinger of the future direction of HIPAA enforcement.

**Risk Management Strategies**

**Technology & Strategy**

It is critical that each health care organization use technology that complements its security policy and 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.

Health care organizations have struggled to combine standards like HIPAA, ISO 27001/27002 (formerly 27799), COBIT, PCI, and their own best practices into a comprehensive framework for information security and privacy. An innovative group called the HITRUST Alliance has created what they hope will
become the industry standard Common Security Framework. The group was formed with input from many industry leaders and is a good resource for those responsible for IT and risk management.

Health care Information and Management Systems (HIMSS) is a not for profit organization dedicated to advancing Health Information Technology. HIMSS provides thought leadership and guidance on a wide variety of Health IT topics.

It’s important for health care providers to ensure that any new technology being implemented has been fully tested and certified. Only six organizations are currently approved to certify that Health IT systems meet meaningful use requirements, including security provisions. One such approved body is Certification Commission for Health Care Information Technology (CCHIT), which was developed jointly by HHS and several leading industry groups in 2004. CCHIT certifies technology vendors and their products for effective use in the health care community and compliance with the meaningful use requirements in the ARRA and is also a great resource for those responsible for HIT procurement.

Contractual Allocation of Risk

An increasing number of data privacy incidents are attributed to business associates – one study found that 59% of 2011 breaches involved external partners, consultants, outsourcers and contractors. Although it is critical to determine the proper allocation of liability when PII/PHI is shared for business purposes, many providers focus largely on compliance with requirements to have a business associate agreement (BAA) in place, rather than maximizing the vendor risk assessment opportunity and risk transfer that a well crafted BAA can provide.

The failure to address these issues proactively can result in confusion and disarray when a breach occurs. Here are two real life examples of outsourced services with breach scenarios that even the most creative risk manager might not have imagined:

- 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 money. Thankfully, this debacle was resolved before the information was exposed.

- More recently, Stanford Hospital & Clinics was brought into a high-profile lawsuit as a result of an outside vendor, Multi-Specialty Collection Services, improperly sharing actual patient data with its marketing vendor, Corcino & Associates. The marketing vendor shared a spreadsheet containing the PHI of 20,000 emergency room patients with a job applicant to test her computer skills. She in turn posted the spreadsheet on a public homework help website, where it was discovered by a patient.
Both were governed by a standard outsourcing arrangement and both highlight the unforeseen 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, or ensuring indemnity for, the health care organization in the unfortunate event of a data breach. While an organization should first rely on pre-negotiated indemnification from the vendor in such a situation, we strongly recommend that insurance requirements be put in place to help ensure that the vendor is able to back up its obligations. We suggest starting with a broadly defined, but specific insurance provision along the following lines:

**Errors & Omissions/Professional Liability Insurance**, in an amount not less than $X,000,000 per claim and annual aggregate, covering all acts, errors, omissions, negligence, infringement of intellectual property (except patent and trade secret); network security and privacy risks, including but not limited to unauthorized access, failure of security, breach of privacy perils, wrongful disclosure, collection, or other negligence in the handling of confidential information, privacy perils, and including coverage for related regulatory defense and penalties; data breach expenses, in an amount not less than $X,000,000 and payable whether incurred by <Client> or <Vendor>, including but not limited to consumer notification, whether or not required by law, computer forensic investigations, public relations and crisis management firm fees, credit file or identity monitoring or remediation services in the performance of services for <Client> or on behalf of <Client> hereunder. The policy shall contain an affirmative coverage grant for contingent bodily injury and property damage emanating from the failure of the technology services or an error or omission in the content/information provided. If a sub-limit applies to any elements of coverage, the certificate of insurance evidencing the coverage above must specify the coverage section and the amount of the sub-limit. Such insurance shall be maintained in force at all times during the term of the agreement and for a period of X years thereafter for services completed during the term of the agreement. <Client> shall be given at least 30 days notice of the cancellation or expiration of the aforementioned insurance for any reason.

Depending on the specific situation, for example if the Business Associate won't be providing a “professional service,” the requirement may be scoped down accordingly. It is critical that companies work collaboratively with legal counsel and insurance professionals to ensure the pieces of the contractual risk allocation puzzle mesh correctly.
Insurance Coverage

All insureds should review their traditional insurance policies to determine the exact scope of coverage for data breaches. However, carriers who offer traditional property and casualty policies are rapidly creating stand-alone Network Security & Privacy Liability (NSP) offerings. In order to promote adoption of these specialized policies, they are inserting more and more broad exclusionary language in traditional policies.

General Liability and Property Policies

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 and 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 Provider 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 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, because only a limited number of carriers will combine the programs.

Other Insurance Policies

Depending upon 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 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 Kidnap and Ransom policies may provide defense and indemnity coverage. In general, such policies were not intended to cover privacy/data breaches and there are significant coverage gaps in each.

Security & Privacy Liability Coverage

Most dedicated policies are provided on a modular basis, so we’ve summarized each module below.

Breach Event Expenses

Triggered by discovery of an privacy incident

This component of coverage provides reimbursement for the insured’s costs to respond to a data privacy or security incident. This module is triggered either by the discovery of such an event, or a statutory obligation to notify consumers of such an event. Covered expenses can include breach-related legal assistance, computer forensics expenses, costs for a public relations firm and related advertising to restore your reputation, consumer notification, and consumer credit monitoring services. Carriers provide
widely varying levels of control and service in this area. Most carriers provide this coverage as a sublimit within the overall policy aggregate, though some offer outside the limit.

**Liability Coverage Parts**

*Triggered by a third party demand or suit*

**Security Liability**

This module covers defense costs and damages suffered by others resulting from a failure of computer security, including liability caused by theft or disclosure of confidential information, unauthorized access, unauthorized use, denial of service attack or transmission of a computer virus. It is almost always combined with the Privacy Liability module below.

**Privacy Liability**

This module covers defense costs and damages suffered by others for any failure to protect personally identifiable or confidential corporate information, whether or not due to a failure of network security. Some policies include: unintentional violations of the insured's privacy policy, actions of rogue employees, and/or the alleged wrongful collection of confidential information.

**Regulatory Proceedings**

This coverage, which is generally a sub-set of the Security and Privacy modules, covers defense costs for proceedings brought by a governmental agency in connection with a failure to protect private information and/or a failure of network security. Coverage is typically sub-limited and may include (depending on insurer) coverage for fines and penalties to the extent insurable by law. Compensatory damages, i.e. amounts the insured is required by a regulator to deposit into a consumer redress fund, may be covered at full limits depending on the insurer.

**Media Liability**

This module can extend the scope of the insured’s personal and advertising injury coverage in a general liability policy. The module covers defense costs and damages suffered by others for content-based injuries such as libel, slander, defamation, copyright infringement, trademark infringement, or invasion of privacy. The scope of covered media is variable and can range from the insured’s website only to all content in any medium.

**Cyber Extortion**

*Triggered by a threat to cause a security failure or privacy breach*

This component, also called Network Extortion, reimburses the insured for expenses incurred in the investigation of a cyber threat and any extortion payments made to prevent or resolve the threat. Payments are generally subject to full discretion by insurer, and insurers offer varying levels of service along with the reimbursement.
First Party Coverage Parts

Business Interruption

This section reimburses the insured for actual lost income caused by a computer network security failure, as well as associated extra expense. Dependent business interruption is also available, but it is often subject to a sub-limit. In addition to a dollar amount retention, a waiting period retention of between 6 to 24 hours is usually applied.

Digital Asset Protection

This module reimburses the insured for costs incurred to restore or recollect intangible, non-physical assets (software or data) that are corrupted, destroyed or deleted due to a covered computer network security failure.

Health care entities considering this coverage should note that the Business Interruption and Digital Asset coverage parts have not been especially relevant to the health care 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 very few first party claims paid by any insurer and significant hurdles to coverage exist, such as waiting periods of 6-24 hours before coverage applies and difficulty in valuing intangible assets and business interruption costs.

Evaluating Coverage Features and Exclusions

Each carrier addresses the risks in a different manner, so it is essential that the insured review the policy form and work with their broker to customize it to their specific exposures. There are many other distinct issues to consider on a case by case basis, but the following basic checklist can be used in the initial evaluation process:

- Does the policy include media liability? Is it broader than our GL policy’s AI/PI grant? Does it contemplate social media exposure?
- How does the policy treat coverage for rogue employees? Employee claimants?
- Will the policy respond if our vendor causes a breach?
- Is there a separate retention for breach response expenses?
- How broad is the regulatory claim trigger? Are fines and penalties covered?
- If we make an acquisition, how does the policy respond?
- Will we be able to use our preferred law firm in the event of a claim? Will their rates be fully covered?
- Does the carrier have a duty to defend? Does it apply to claims as well as regulatory actions?
- What exclusions exist for breaches that we aren’t aware of, but may already be ongoing?
- When do I provide notice of a claim or incident, and what qualifies as a covered claim?
- Does the policy exclude unencrypted or unprotected data or devices?
What other exclusions should we be specifically concerned about, and what corresponding uncovered claim scenarios could arise?

Breach response expenses are perhaps the most differentiated area of coverage, and a specific set of questions apply to that element:

- Is the trigger a reasonable belief that identity theft may occur as a result of a particular incident, or is it tied to statutory obligations only?
- Does the policy only pay those costs the insured is required to incur by law or does it provide for voluntary expenses such as providing credit monitoring in a state where the law does not require it?
- Is the insurer’s prior written consent required before coverage will apply? Is there a reasonableness standard for consent?
- Are costs incurred solely to mitigate damage to the insured’s reputation covered?
- What time constraints apply? Can the insured recover costs under this coverage part more than one year after a breach?
- Does coverage apply on a per individual basis or is a set dollar amount available?
- Does coverage erode the available limit of liability or is it provided outside and in addition to the limit?
- Do the covered expenses mesh with the insured’s crisis response plan? Are the insured’s preferred crisis management vendors pre-approved?

Insurance Marketplace & Benchmarking

The market for Security and Privacy Liability remains competitive, with favorable risks with clean loss history renewing flat, and carriers continuing to solicit new insureds. Many experienced markets have now paid large claims and regulatory costs, and are becoming more inquisitive in their underwriting process and wary of taking on insureds without state of the art controls.

Benchmarking in this area is of limited value as it is difficult to categorize insureds and because each underwriting situation is based on many different factors such as revenues, patient statistics, loss history, information security posture, contractual allocation of liability and number/accessibility of data records. Many forward looking health care entities are basing their limit and retention decisions on data breach cost modeling, such as the ID Experts PHIve7 method, which quantifies the value of PHI for both risk transfer and IT security investment purposes, or on modeling based on peer loss experience.

There are at least fifteen carriers that can provide a primary program for health care entities, with capacity to build in excess of $100,000,000 in total limits. Retentions generally fall in the $250,000 - $500,000 range, but can be as low as $10,000 or as high as $10,000,000 depending on risk tolerance and exposure. Pricing for a stand alone program varies widely but usually falls within a range of $10,000 to $35,000 per million of coverage. Very large organizations or those with weaker security and privacy controls may be forced to take higher retentions and pay premiums in excess of $50,000 per million.
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
- 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

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.
Contact Information

Sarah Stephens  
Vice President  
Aon Risk Solutions  
Financial Services Group – Professional Risk Solutions  
199 Fremont, Suite 1500  
San Francisco, CA 94158  
t +1.415.486.7438  
sarah.stephens@aon.com

How to cite this publication

Individuals are encouraged to cite this report and any accompanying graphics in printed matter, publications, or any other medium, as long as the information is attributed to the cited source or to Aon plc.

About Aon

Aon plc (NYSE: AON) is the leading global provider of risk management, insurance and reinsurance brokerage, and human resources solutions and outsourcing services. Through its more than 61,000 colleagues worldwide, Aon unites to empower results for clients in over 120 countries via innovative and effective risk and people solutions and through industry-leading global resources and technical expertise. Aon has been named repeatedly as the world's best broker, best insurance intermediary, reinsurance intermediary, captives manager and best employee benefits consulting firm by multiple industry sources. Visit www.aon.com for more information on Aon and www.aon.com/manchesterunited to learn about Aon's global partnership and shirt sponsorship with Manchester United.

1 “Breach Report 2011; Protected Health Information” www.redspin.com
2 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html
3 http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html
5 http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=3120
6 “Protecting PHI and Responding to Data Thefts,” Davis Wright Tremaine LLP, Randy Gainer and John McGrory
7 http://www2.idexpertscorp.com/resources/white-papers-and-studies/ANSI-PHI-Project/