Wortham

Insuring the Future
Since 1915

Management Liability Policies

How Do They Provide Protection for Healthcare Executives and Healthcare Systems

Presented By: Lori Wheeler, Managing Director

TAHFA

Cyber Risk - Do You Have It?

Nearly every organization, regardless of industry, has an exposure to cyber risk, as we live and work in a digital world. Even if an organization does not maintain sensitive data about its clients or customers, most businesses retain personally identifiable information (PII) in some form or another about their own employees. If an organization offers health insurance and medical benefits, protected health information (PHI) may be on hand and that needs to be protected. Additionally, with many organizations moving towards paperless operations, important data that is crucial to running a business often rests within a computer network.

Every Company Faces the Risk of Cyber Liability

What happens if this data is compromised in a cyber security breach? A growing list of regulations governing the unauthorized use of protected and sensitive information may impact the organization by way of regulatory proceedings, fines, or penalties. The threat of lawsuits by parties whose information has been compromised is on the rise and the cost of responding and remediating a breach can be detrimental to an organization. A cyber breach can also cause communication and operational disruption for an organization, as well as potential reputational damage to the business.

Are You at Risk? It's Time to Rethink Your Position on These Risks and Exposures

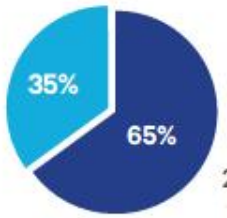
In order to determine if cyber risk is an area for you to be concerned, here are some key questions to ask within your organization:

- Do you maintain personally identifiable information, personal health information, or other sensitive or confidential information on your computer network?
- Do you use outside vendors to host or manage any of your IT network including HR functions, payment processing, or cloud services?
- Do you rely on your computer network to run your day to day business? If your network were to be disrupted via a security breach, how would this affect your ability to generate continued operations?
- Do you know who you would reach out to in the event of a security or privacy breach to your computer network (legal advice, forensic accountants, public relations firms, crisis management, breach response services)?
- How will your traditional property and casualty policies address cyber risk?

Your Account Executive at Wortham can help you navigate through this exposure to determine if a Cyber Insurance Program is right for you.

Data shows nearly 50% of users open e-mails and click on phishing links within the first hour.

Source: 2015 Verizon Data Breach Investigation Report.



65% of respondents purchased cyber insurance in 2015 compared to 35% in 2011.

Advisen October 2015 Survey; Information Security and Cyber Liability Risk Management

Cyber Risk Coverage

A well crafted cyber insurance policy will generally address the expenses associated with a cyber breach. Most policies will cover the costs associated with hiring attorneys and forensic IT experts, notifying customers, providing annual credit monitoring, as well as provide reimbursement for state or federal fines or penalties. Manuscript language is available for those organizations warranting specialized coverage.

Third Party Liability Coverages	Coverage Description
Privacy and Network Security Liability	Protection for liability arising out of allegations of security and privacy wrongful acts against the Insured. Damages and claims expenses incurred as a result of a covered claim are included.
Regulatory Defense and Penalties	Protection for those amounts Insured is obligated to pay arising out of certain privacy regulatory actions. Defense costs and certain fines/penalties included.
Media Liability	Protection for liability arising out of allegations of multimedia wrongful acts, such as allegations of libel, slander, invasion of privacy, emotional distress, mental anguish - all in connection with the Insured's multimedia.

First Party Coverages	Coverage Description
Notification Expense/Credit Monitoring	Reimburses Insured for first party notification expenses incurred by the organization following a privacy or security breach. May extend to credit monitoring services, call center services, and other event management response expenses.
Network Interruption and Data Asset Restoration	Reimbursement for loss of net income and extra expenses following a security breach; also provides reimbursement for reasonable costs to restore, replace or reproduce damaged or destroyed computer programs, software and electronic data.
Extortion Expenses	Money and expenses paid at the recommendation of an approved service provider relating to cyber extortion demands.

Additional Coverages Available in Select Policies

Computer Fraud / Electronic Fraud / Social Engineering Fraud

Reputational Harm

Professional Liability Errors & Omissions

Cyber Litigation

Overview:

- Hospitals face a unique challenge when it comes to providing security for their clients' data: the data must be easily accessible so medical personnel are able to administer treatments quickly while also secure, as much of their clients' information is extremely sensitive.

- According to a recent study[1] data breaches that include Personal Medical Information (PMI), have a high probability of settling in favor of the plaintiffs should the incident go to court; primarily due to the sensitive information leading to emotional and other damages.

[1]*Empirical Analysis of Data Breach Litigation,* Romanosky et.al., February 2012
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1986461

Cyber Litigation

- **South Shore Hospital**[1] was fined $750,000 by Massachusetts' Attorney General when some unencrypted backup records were lost in shipping, exposing 800,000 patients' PMI and financial records.

- **West Virginia University Medical Corporation**[2] was forced to pay $2,300,000 in punitive damages when an employee took three women's mental health records home and discussed them with locals.

[1] http://www.eweek.com/c/a/Health-Care-IT/Massachusetts-Hospital-Agrees-to-750000-Settlement-in-Data-Breach-Lawsuit-463340/

[2] www.hipaadivsory.com: *WV Jury Awards Millions to Victims of Privacy Breach*

Cyber Litigation

- **Emory Hospital**[1] was served with a class action lawsuit alleging $500,000,000 in damages for losing 10 data disks containing sensitive personal data of over 315,000 patients

- **The Sutter Health Foundation**[2] A class action suit seeking $1,000 for each of the effected 4.3 million patients was filed against after a laptop containing PMI was stolen from their hospital.

- **UCLA Healthcare System**[3] had to defend itself in a case that alleged up to $16 million in damages following a data breach. The incident occurred when a doctor brought a hard drive home and subsequently had it stolen during a break in, exposing 16,288 patients' personal information.

1 http://www.beckershospitalreview.com/legal-regulatory-issues/emory-healthcare-faces-class-action-suit-over-data-breach.html
2 http://www.sacbee.com/2011/11/23/4074676/sutter health_sued over theft.html
3 http://www.californiahealthline.org/articles/2011/12/22/class-action-lawsuit-filed-over-ucla-health-system-data-breach.aspx

Cyber Regulatory Violation

- In 2015, Cancer Care Group, P.C. agreed to settle potential violations of HIPAA with the OCR. Cancer Care paid $750,000 and agreed to adopt a robust corrective action plan to correct deficiencies in its HIPAA compliance program. Cancer Care notified OCR that unsecured electronic protected health information was potentially released after a laptop was stolen from an employee's car. The laptop contained names, addresses, dates of birth, Social Security numbers, insurance information and clinical information for approximately 55,000 current and former patients.

Cyber Breaches:
Missing Portable Device (unencrypted)

Unencrypted backup tapes were lost that contained 1.6 million pediatric patients billing information on them including names, DOBs, SSNs, diagnosis codes, health insurance information. The tapes also included employees, physicians and vendors information totaling 200K people. The tapes were believed to have been lost during a remodeling project in the IT department.

CYBER LIABILITY RESPONSE:
The entity used mail vendor, call center, credit monitoring, legal, forensics and crisis management. There was an OCR investigation that lasted 3.5 years and was ultimately dismissed.

Cyber Breaches:
Insider (social media policy violation)

A healthcare organization's employee posted patient treatment information on a social media website. The employee did not include the patient's name, but because the disclosure occurred in a small town, the public could determine the patient's identity.

CYBER LIABILITY RESPONSE:
Insurer connected the organization to expert privacy legal counsel, who provided advice on notification to the individual, as well as satisfying the necessary regulatory response.

Cyber Breaches: Hacking/Malware (phishing)

Sophisticated foreign phishing attack exposing information in email boxes of nearly 20,000 pediatric patients. Employees clicked on the phishing emails and either gave up credentials or launched malware into their network. Forensics found some evidence of data exfiltration. The data contained patients' names, clinical information, phone number, addresses, insurance information and some social security numbers.

CYBER LIABILITY RESPONSE:

Patients notified utilizing outside legal, forensics, notification and call center vendor, and credit monitoring. OCR investigation is pending.

Cyber Breaches:
Inadvertent Disclosure (unsecured online file)

IT vendor had inadvertently unsecured a file containing over 30,000 patients billing information such that it was searchable on the internet using Google and the like. The hospital discovered the incident during security testing when a larger system acquired it. Information exposed included names, SSN, DOB, address, treatment information, and insurance information.

CYBER LIABILITY RESPONSE:
Hospital utilized outside legal, forensics, mail and call center, credit monitoring and crisis management. Investigated by OCR and 4 attorneys general.

Cyber Breaches: Insider

Hospital employee was stealing patient information and selling to local crime ring to file fraudulent tax returns. Hospital was advised of this by law enforcement. Began an investigation and 115,000 patients were notified. Information included names, SSN, DOB, address and treatment information.

CYBER LIABILITY RESPONSE:
Hospital used outside forensics, legal, mail and call center, credit monitoring and crisis management. OCR investigation pending after 3 years. Class action lawsuit filed but was dismissed.

Crime Coverage

- Loss of money, securities and other property resulting from dishonest acts committed by an employee
- Loss from forgery or alteration of checks or similar documents
- Loss of money and securities inside the premises resulting from theft, disappearance, or destruction
- Loss of money, securities and other property outside the premises while in the care of a messenger
- Loss of money, securities and other property resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the premises or banking premise to a person or place outside those premises
- Loss resulting from acceptance of money orders that are not paid upon presentation or counterfeit currency
- Loss of funds from a fraudulent instruction directing a financial institution to transfer, pay, or deliver funds from your transfer account
- Loss resulting from having transferred, paid or delivered any money, securities or other property as the direct result of Social Engineering Fraud committed by a person purporting to be a vendor, client or employee who was authorized to instruct other employees to transfer money, securities or other property

Social Engineering Loss

- An employee received an email that appeared to be from its CFO, requesting a wire transfer to a bank account in China. The email stressed the urgency and also the need for secrecy regarding the transaction. When the employee placed a call to the CFO the next day in order to find out how the payment should be coded for reconciliation purposes, it was discovered that the CFO's email had been hacked and the request was fraudulent.

Social Engineering Loss

- An employee received an email that appeared to be from its CFO, requesting a wire transfer to a bank account in China. The email stressed the urgency and also the need for secrecy regarding the transaction. When the employee placed a call to the CFO the next day in order to find out how the payment should be coded for reconciliation purposes, it was discovered that the email address used was not the CFO's and the request was fraudulent.

Social Engineering Loss

- A hospital purchased 1,000 laptops from its supplier. Payment for the order was due to the supplier within 45 days. A few weeks after receiving the shipment of laptops, the hospital received an email purportedly from the supplier providing revised bank account information for payment of the invoice. The hospital updated its accounts receivable and issued payment using the new banking instructions. Subsequently, the hospital received an inquiry from the actual supplier regarding the status of the payment. The supplier's email system was hacked, and the change to the supplier's banking instructions was fraudulent.

Employee Dishonesty

- After a hospital placed a legitimate order with its pharmaceutical wholesaler, technicians would use a pharmacist's password to make an illegal purchase. Once the wholesaler approved it, they would erase the second order from the computer systems. Both orders would arrive at the same time, but with separate receipts. The technicians would hide the paperwork from their portion and cart it away.

- The scheme may have gone unnoticed for longer had the hospital not changed its financial accounting system, which helped administrators catch the suspicious spending within a month. The hospital did not release how much money it lost, but it is estimated to have easily cost millions of dollars.

Employee Dishonesty

- A nurse admitted to stealing hydrocodone, oxycodone and hydromorphone from his rehab center employer. He recorded that he had given the drugs to his patients when in fact he was ingesting them himself, “often while still at work.”

- A nurse anesthetist regularly stole liquid opioid medications for his own use. According to documents from the licensing department, he collapsed in the operating room while performing a general anesthesia procedure and tested positive for fentanyl, meperidine and normeperidine.

Kidnap & Ransom

- Hospitals and healthcare facilities have to manage a wide range of complex security threats. As institutions that are open to the public 24-hours a day, such facilities are exposed to incidents of violence, cases of child abduction and threats of extortion. As a result of these risks, security in hospitals has become paramount and significant measures such as closed circuit television, regular security patrols and even a police presence have become commonplace.

- Unfortunately, traditional security methods are no longer enough to adequately protect healthcare facilities against complex risks such as child abduction, extortion and workplace violence. Incidents that do occur are emotive, often widely publicized and can lead to costly lawsuits. Affected parties may seek to hold a facility accountable for situations that occur on its premises, citing inadequate security or lack of an immediate and effective response to a crisis.

- Hospitals must carefully consider the security of their maternity units in order to protect mothers and their newborns. Institutions often need to employ additional security measures to protect staff and patients from threats of extortion or violence.

Kidnap & Ransom Coverages

Expenses incurred in responding to:

- Abductions of infants or children including abductions by the non-custodial parent
- Threats of violence against staff, volunteers or management
- Threats of damage to property

Extortion threats to:

- reveal confidential or proprietary information
- kill or injure insured persons
- damage property
- disrupt computer systems
- contaminate medical supplies
- Hijackings of ambulances or other vehicles
- Hostage situations involving patients or staff
- Kidnaps for ransom
- Disappearances

Abduction

- A new mother sat in her room in a secure and well-managed private hospital feeding her newborn baby. A woman in a nurse's uniform came into the room and told the mother she was taking the baby for tests. The mother handed the infant over and, within minutes, the infant was out of the hospital, abducted by the woman who had been impersonating a nurse.

Violence

- A disturbed man whose father died during surgery at a community hospital blamed the staff and threatened retribution. Three days later he walked into the emergency ward and fired a small-caliber handgun, killing a nurse,
- an emergency medical technician, and wounding the physician.

Parental Abduction

- Following charges of child abuse and neglect, a father attempted to abduct his son from a hospital where the baby was being cared for while in the custody of social services. The father hid his infant son in a cloth bag, walked out of the hospital's seventh-floor nursery and made his way to the street via an emergency exit.

Extortion

- A medical center received an extortion demand from a staff member. The technician threatened to publicly claim he had given patients HIV-contaminated blood unless he was paid $1 million.

Directors & Officers Liability

- Side A: insurer shall pay the loss of insured persons for which the insured persons are not indemnified

- Side B: insurer shall pay the loss of the organization for which the organization has indemnified the insured persons

- Side C: insurer shall pay the loss of the organization

  - For claims for Wrongful Acts
  - defined as actual or alleged error, omission, misleading statements, neglect, or breach of duty

Antitrust Claim

- Stealth, a group of doctors who owned and operated a surgical hospital, argued among other things, that Memorial Hermann used its might to scare insurance companies away from doing business with the smaller hospital. The doctors said Memorial Hermann violated antitrust laws by secretly coercing health insurers to strangle the startup hospital's business. Their attorney, Rusty Hardin, had characterized the case as “Goliath going in there and trying to run David out of business.” He said the smaller hospital's doors closed in 2006, after about a year and a half, because Memorial Hermann improperly threatened to raise prices or pull business from health insurers who worked with the smaller hospital. Memorial Hermann officials have said they did nothing wrong and sometimes a nonprofit has to play business hardball to be able to stay healthy itself.
- The lawyer for Memorial Hermann has said his client was reasonably concerned about business it could lose to the new hospital. “Whether a medical institution is profit or nonprofit, it has to survive. The way you survive is to compete — fairly and aggressively,” the lawyer stated.
- This is Memorial Hermann's second settlement of a lawsuit over its aggressive tactics with insurance companies that might have done business with the startup competitor hospital. In January 2009, Memorial Hermann settled a separate lawsuit in which Texas Attorney General Greg Abbott alleged the institution organized an insurer boycott to keep Stealth’s hospital from succeeding. Memorial Hermann did not acknowledge any wrongdoing but agreed to pay the state $700,000 toward the cost of the antitrust investigation and agreed to not take the same type of anti-competitive actions alleged in the lawsuit for five years.
- It is rumored that Memorial Hermann paid over $50,000,000 to settle the antitrust claims from Stealth.

Houston Chronicle January 11, 2010, Memorial Hermann Settles Part of Antitrust Lawsuit

Peer Review/Credentialing Claim

- In May 1998, interventional cardiologist Lawrence R. Poliner, MD, performed an angioplasty on a patient experiencing a heart attack. Poliner opened one partially blocked artery, and allegedly, did not notice another major artery was completely blocked. Following this procedure, the patient was admitted to the intensive care unit with shock and respiratory failure. This outcome was later reviewed by the Internal Medicine Advisory Committee of Presbyterian Hospital in Dallas. After consultation with hospital administration, the chief of cardiology and the director of the cath lab, the committee offered Poliner a voluntary, temporary restriction of his catheter lab privileges pending further investigation. This temporary restriction of selected privileges was called an “abeyance” under the hospital staff bylaws. The alternative for Poliner was a formal suspension. Poliner requested consultation with a lawyer, but was denied, in the interest of time. He agreed to the voluntary restriction of his privileges, i.e., the abeyance and retained counsel.

Peer Review/Credentialing Claim

- Presbyterian Hospital appointed a team of cardiologists to review 44 of Poliner's cases. The team found evidence of substandard care in more than half of the cases. The voluntary restriction of privileges was continued for almost 30 days while the committee requested additional time to investigate. The committee unanimously recommended that Poliner's echocardiography and catheter lab privileges be suspended, because of substandard patient care and poor physician judgment. A few months later, a hospital panel agreed that Poliner's suspension of privileges was justified based on the data available to the committee at the time, but reinstated certain privileges with conditions.

Peer Review/Credentialing Claim

- Poliner brought a lawsuit against Presbyterian Hospital and the doctors involved in his peer-review process. Poliner alleged the peer-review proceedings were defective and conducted in bad faith by his business competitors, i.e., other cardiologists. Specific legal claims included defamation, federal and state antitrust claims, breach of contract and violations of the Texas Deceptive Trade Practices Act.

- The jury found for Poliner and his professional association on the abeyance-related claim. The verdict was more than $360 million in damages, including $90 million for deformation and $110 million in punitive damages. Time magazine covered this case, from the perspective of the plaintiff, stating that Poliner prevailed against a hospital where three colleagues had trumped up charges of substandard care against him to eliminate Poliner as a competitor.

Orthopedics Today, December 2013
B. Sonny Bal, MD, JD, MBA; Lawrence H. Brenner, JD

Tax Status Litigation

- In November 1990, the Texas Attorney General filed a lawsuit against The Methodist Hospital System, alleging that it had failed in its duty to provide enough charity care to poor people. The state claimed that the hospital provided significantly less charity care than the hospital reported; it then filed the suit in an effort to require specific performance--that is, to compel the hospital to provide greater amounts of charity care in the future. The case focuses on the amount of charity care provided before the suit, the economic value of the tax exemption provided to the hospital because it is a not-for-profit (NFP) hospital, and the responsibilities of the hospital given the expectations of society.

Employment Practices Liability

Claims alleging

- Discrimination
- Harassment
- Hostile Work Environment
- Wrongful discharge
- Breach of employment contract
- Defamation/libel/slander
- Failure to enforce policies
- Emotional distress/mental anguish
- Retaliation
- Negligent evaluation
- Negligent hiring/supervision/training
- Failure to promote or grant tenure

Class Action Litigation

In the mid 2000s, the nation's anemic supply of nurses is a familiar headache for recruiters or executives who grapple with hospitals' daily operations and budget. Now it's an issue for hospitals' general counsels as well.

Lawsuits in a handful of states allege that hospital executives conspired to hold down wages amid a national nursing shortage, just when economic theory says demand should be pushing pay upward. Separately, legal action against a California hospital trade group contends the association helped hospitals collude to illegally fix overtime wages despite demand.

At stake are millions of dollars in alleged lost wages if judges in Albany, N.Y.; Chicago; Detroit; Memphis, Tenn.; and San Antonio grant plaintiffs class-action status.

Nurses' yearly wages fell thousands of dollars short of where they should have been, lawyers contend. In Albany that amounted to $6,200 per nurse, per year; in Chicago it was $5,400; in Detroit, $5,000; and in Memphis, a whopping $14,100 per nurse, according to initial estimates, says Daniel Small, a Washington attorney with Cohen, Milstein, Hausfeld & Toll, who is representing nurses in all five cities. Even in San Antonio, the city with the lowest estimated losses, nurses' wages were depressed by $1,334 per nurse annually, preliminary figures from the lawyers show.

Lost wages in three cities could total at least $376.9 million, based on the plaintiffs' estimate of how many nurses worked in Albany, Memphis and San Antonio in 2005 and the percentage who were employed by defendants. In Detroit, rough estimates of the nursing workforce could put losses as high as $200 million. No estimates were available for Chicago.

The lawsuits, filed since June 2006, name 73 hospitals and 16 health systems and allege hospital executives agreed to regularly swap nonpublic figures on pay and anticipated raises for nurses and agreed not to compete on compensation. The lawsuits contend that hospital officials relied on informal and commercial wage surveys and professional meetings to exchange information on nurses' compensation, anticipated raises and bonuses.

The defendants rejected the claims. Employers contend they set nurses' pay and benefits independently using legitimate, competitive compensation strategies, according to court filings. Lawsuits fail to cite direct evidence of a conspiracy for actions that could just as easily be competitive, note attorneys for Baptist Health System based in San Antonio.

Sexual Harassment

- Three surgical nurses accused a surgeon of sexual harassment arising from one incident in the surgical suite. The surgeon allegedly picked up a surgical instrument and asked the nurses if they would like to see his “instrument.” Each nurse received $300,000 in settlement from the hospital who employed them.

Retaliation

- A federal jury awarded more than $500,000 to a former Covenant Medical Center employee, finding that her termination from the hospital was retaliation for taking medical leave. An eight-person jury determined Covenant Medical Center violated the Family and Medical Leave Act and the Americans with Disabilities Act when it fired 41-year-old Amanda Perry in November 2014.
- After working as a biller, Ms. Perry, who had a history of psychiatric diagnoses, was promoted to office coordinator of two of Covenant's physicians' offices in 2012. In July 2014, Ms. Perry's symptoms related to her psychiatric diagnoses worsened. She subsequently requested a leave of absence as a result of her medical condition. According to court records, she took several days off between July 25, 2014, and Aug. 15, 2014.
- In August 2014, Ms. Perry's supervisor allegedly expressed concerns about the amount of time Ms. Perry was taking off from work and told her "to get it together." Ms. Perry remained off work from Aug. 15, 2014, through Oct. 6, 2014.
- When she returned to work she was reassigned as the coordinator for two primary care clinics. A few weeks later, she received a "step I" discipline for behavioral and performance issues. She subsequently received a "step III" discipline — a final warning — for unprofessional conduct and crying in front of a patient. Ms. Perry was effectively fired when she received a "step IV" discipline for allegedly asking a co-worker to provide a false statement.
- Although the hospital claimed Ms. Perry was fired for the issues identified in the disciplinary warnings, Ms. Perry said she was let go because she requested time off and due to her disability. The jury awarded Ms. Perry more than $30,000 in back pay, $445,000 in front pay and $25,000 for mental anguish. In addition, Covenant is responsible for attorney fees, which are about $100,000.