The collecting, sharing and transmitting of information is vital to any healthcare encounter. As anyone working in the healthcare industry knows, there has been an increasing demand for more and better data to aid in the provision of service, to facilitate performance evaluations and to substantiate reimbursement. Much of the data collected is highly sensitive, relating to an individual’s medical or financial information. Any of this type of information in the wrong hands could cause personal, emotional and financial harm to an individual who had a legitimate expectation of privacy and security when providing the information.

In the healthcare environment, data is generated by many different members of the healthcare team and its accuracy and appropriateness is not always verified. In addition, the migration of data from a paper-based form to an EMR (electronic medical record), EHR (electronic health record) or other digitized format now allows healthcare data to be more easily transmitted from provider to provider, site to site or to external regulatory and billing entities. In order for this data to be secure, appropriate encryption and security must be established for all senders and all receivers of the data.

The emergence of telemedicine and telepsychiatry, where sensitive medical and psychiatric information is shared over the phone or the Internet, can also give rise to liability, if any of these modes of communication are hacked or if information passing from one provider to another is intercepted.

Finally, websites which have been developed by healthcare organizations for marketing and branding purposes include increasing amounts of information and intellectual property. In addition, the use of these sites for multiple purposes and the amount of content available continues to grow. The sophistication of these sites, and what can be accessed through them, poses unique risks and challenges along with potential business opportunities. They must be continually assessed to maintain their security and assure all content is appropriate.

Each of the exposures described above can give rise to cyber liability claims which have as their basis: breach of privacy, infringement of intellectual property rights, fraudulent billing and other exposures.

*The Emergence of Cyber Liability as a Cause of Action in Other Industries*

In other industries (banking, publishing, credit card, etc.), problems associated with fraudulent access to personal information often followed by the misuse of that information, has been well documented and laws have been enacted in response. “According to Privacy Rights Clearinghouse, over 263 million data records of U.S. residents have had some form of security breaches...
since 2005.” Advisen contends, “Modern technology enables massive amounts of information about individuals to be gathered, processed and transmitted. But software vulnerabilities are pervasive. Surveys by Ernst & Young and the Computer Security Institute (CSI) reveal that 90% of businesses and government agencies have detected security breaches and 75% recognized financial losses from the breach.”

Legal costs have risen not only to pay verdicts or settlements from claims alleged against the organization, but also to pay for the costs of defense of claims brought by third parties for allowing, or failing to prevent, unauthorized access to sensitive information.

**Cyber Liability: An Emerging Risk in Healthcare**

Healthcare as an industry is not immune from cyber liability. In fact, given the personal nature of the information stored, the evolution of EHR/ EMR systems, the growth of telemedicine, the increase of e-mail for communicating information that historically has only occurred through face to face encounters, and the number of entities now requesting and receiving healthcare data electronically, there is no doubt this exposure is one risk managers, compliance officers, IT professionals, providers and all members of the leadership team need to be mindful of. Careful planning, strategic risk financing, focused education, and constant vigilance can all help to manage this exposure.

**What is Cyber Liability?**

**Cyber Liability** is composed of two defined risks:

1. **Security Liability** is the unauthorized access/use of a utility’s (or vendor/partner/independent contractor) network. In 2007, the exposure involved the theft of mobile computer equipment such as desktop servers or a laptop to perpetrate data theft. It is well known that many cases involve employees who have trusted access into the network. Employees or trusted third parties with access into the network can steal identity information, critical business information, transmit malicious code, and participate in a denial of service attack against your network or the network of others. This risk includes paper documents, as well as electronic data.

2. **Privacy Liability** is the violation of privacy laws or regulations that permit individuals to control the collection, access, transmission, use, and accuracy of their personally identifiable medical and/or financial information. The most serious civil and regulatory exposure surrounds personally identifiable non-public information; however, there are risks associated with disclosure or theft of confidential corporate data of others.

**Cyber Crime: A Clear and Present Danger**, an excellent white paper released by Deloitte and Touche LLP’s Center for Security and Privacy Solutions, reported and analyzed key findings from the 2010 annual CSO survey. Deloitte shared their thoughts about the rise in this type of crime and outlined the steps organizations can take to protect themselves from liability.

As related specifically to their assessment of the prevalence of cyber liability, Deloitte maintains:

1. Cyber crime is now serious, widespread, aggressive, growing and increasingly sophisticated and poses major implications for national and economic security.

2. In many industries, institutions and public and private-sector organizations (particularly those within the critical infrastructure) are at significant risk.

3. Relatively few organizations recognize organized cyber criminal networks, not individual hackers, as their greatest potential cyber security threat. Even fewer are prepared to address this threat.

4. Organizations tend to employ security-based, “wall-and-fortress” approaches to address the threat of cyber crime, but this is
not enough to mitigate the risk.

5. Risk-based approaches—and approaches that focus on what is the IT environment, going in and out of—hold potentially greater value than traditional, security-based, “wall-and-fortress” approaches.

6. Organizations should understand how they are viewed by cyber criminals in terms of attack vectors, systems of interest, and process vulnerabilities so that they can better protect themselves from attack.

Although the report does not specifically address cyber liability in the healthcare industry, it provides a risk-based approach that can be adapted to some of the unique risks inherent in healthcare. In addition, it emphasizes the need to develop actionable intelligence, which includes asking the following six questions:vi

1) How can we improve our visibility into the environment?
2) What new technologies do we need to watch for and monitor?
3) Do we have vulnerable technologies and data?
4) To what extent will our existing controls protect us?
5) Which industries are cyber criminals targeting and which techniques are they using and planning to use?
6) How can we identify actionable information?

The report goes on to describe the benefits of such a risk-based approach when it is integrated into an enterprise risk management strategy.

**Cyber Liability Claims in Healthcare**

Data security breaches in healthcare can result in losses from a number of sources. Hospitals, healthcare organizations and provider groups may incur fines or penalties if they are not in compliance with privacy and data security laws, such as HIPAA. In addition to the personal damages that may be demanded, a breach can also result in millions of dollars in expenses for repairing the breach, tightening security measures, notifying patients of the actual or potential breach and mitigating damages. Loss of trust and other reputational damages can have a significant impact on the level of trust patients and providers have in the institution. In extreme cases, it can be ruinous. Lawsuits by patients, providers and business partners can result in millions of dollars in settlements.

In healthcare, many very public exposures have already been reported.vi

1. A health system accidentally posted the medical records of thousands of patients on the Internet. A class action suit was filed for alleged emotional distress of the affected patients. The class action seeks damages in excess of $10 million and the federal government has notified the system to prepare for an investigation under HIPAA.

2. A woman purchased a used computer from a pharmacy. The computer still contained the prescription records, including names, addresses, social security numbers, and medication lists of pharmacy customers. The cost of notifying affected parties per state law totaled nearly $110,000. Two lawsuits have been filed: one alleges damages in excess of $200,000 from a party who claims she lost her job as a result of the disclosure; the second alleges the plaintiff’s identity was stolen, and the costs of correction and emotional distress will exceed $100,000. A HIPAA investigation is also underway.

3. A part-time hospital employee gained unauthorized access to confidential electronic patient records and discussed an individual’s HIV status with co-workers. The individual sued the hospital for lack of adequate IT security measures in
What is Cyber Liability Insurance?

The rate of development of privacy and data security insurance products has been hampered by the fact that buyers were frustrated by the patchwork of non-standardized coverages and comparatively low limits available in the market. At the same time, insurers have been less than enthusiastic about developing products with significant underwriting challenges for which there was a perceived lack of demand. Without an adequate claims history, it is often difficult to fully understand the types of exposures and to underwrite them with any precision. As more exposures have been reported and the risks become better understood, many carriers have entered the marketplace with comprehensive policies. Companies now offering cyber liability products include AIG, Chubb, Travelers, Ace, CNA, Darwin, Beazley, Hiscox, Zurich, Evanston and Great American. As underwriters, both at the primary and reinsurance levels, become more familiar with these exposures and their financial costs, coverage is likely to be further refined. In addition, as risk reduction efforts become more sophisticated and proactive, it is likely that policy limits will increase, pricing will become more competitive and products will be better tailored towards specific types of exposures.

At the present time, cyber liability insurance can safeguard your organization against claims arising from:

**Business Interruption:** Lost income from a computer attack or other non-physical peril.

**Network Security:** Damages arising from a computer attack on your network.

**Internet Liability:** Damages from your Internet service provider going down or being hacked.

**Web Content Liability:** Damages and defense costs stemming from claims of libel, copyright or trademark infringement, or defamation; damages to a website by a hacker or disgruntled employee.

**Electronic Communications:** Damages and defense costs arising as a result of electronic communications, such as breach of confidence or infringement of any right to privacy, intellectual property rights or any statutory duty. (Example: some states now require organizations to notify those affected by a loss of private information and provide them credit monitoring services at the organization’s expense.)

**Intangible Assets:** Damages to code, data, etc.

All organizations are at risk for some type of data exposure. In addition to the most common claims that relate to hacking into financial information, it is clear that personal information about an individual’s health warrants an even higher degree of protection. Though many have touted the value of digitizing health records to allow for greater accessibility of patient information, this accessibility clearly has some risks.

Healthcare organizations and provider groups need to be investing in technologies that assure security and establish policies that educate staff as to their responsibilities in safeguarding data privacy.

Strategic / Proactive Risk Management Strategies for Identifying and Managing Cyber Liability Threats in the Healthcare Environment

There are a number of crucial steps a healthcare organization can take to protect itself from cyber crime. The process of risk control in this area requires initial assessment of present risk, mindfulness of emerging risk and proactive management of all aspects of technology that exist in the organization to facilitate data transmission while maintaining security in the process. Controlling cyber liability is not an activity that should be relegated to a single department and must include all key stakeholders. Strategies that might be particularly suitable for the healthcare environment include:
1. **Conduct an environmental scan to identify the types of cyber risk that might be inherent in your organization.** Be mindful of the following activities and assess the risks and the benefits associated with each.

- Many organizations are converting paper-based medical records into electronic health records. The process, however, is not always well thought out or consistent throughout the organization.
- Different systems may be used in different departments (particularly in a large organization or a healthcare system with multiple sites of care).
- Integration and connectivity issues may be complicated if multiple vendors are used and security promised by one system may not be guaranteed as data from one system is transferred to another.
- Providers are increasingly using handheld devices and computers to store and transmit data and to communicate with colleagues and patients.
- If your organization or your providers are engaged in telemedicine, make certain you carefully assess the technology being used to facilitate those consults. If you are anticipating establishing telemedicine programs, use appropriate due diligence to create a secure network.
- Marketing departments are more aggressively using their company’s websites and social media sites to promote activities of the organization.
- Management staffs are using the internet to transmit sensitive clinical and financial data to external payers and regulators.
- New technology purchases may serve to add to the risks of the organization.

2. **Be proactive in designing policies and practices that minimize the risk of cyber liability.** The responsibility for maintaining patient privacy and network security extends beyond the information technology (IT) department. There should be a team approach with members of risk management, finance, IT, human resources (HR), billing and compliance that meets regularly to develop and monitor policies and protocol to promote an enterprise-wide approach. The policies should address financial, privacy, and security concerns. Clearly defined policies would be beneficial in the following situations to help minimize the risk of cyber liability.

- Any individual in the organization who has responsibility for entering, accessing or transmitting data should be aware of risks associated with using an electronic capture system for entering and transmitting data.
- Personal handheld devices and smart phones now have applications which display x-rays and other scans; individual providers may use these devices to send their interpretation of these tests to others outside the secure hospital network. Policies must be strict in their prohibition of using personal devices to store or send sensitive patient information.

3. **Work closely with your compliance department to fully understand the privacy concerns raised by HIPAA and the HITECH act which may be unique to the healthcare setting.** Verify that those concerns are fully addressed as related to employees, vendors, consultants and anyone who might have access to, or receive data from, the organization.

4. **Utilize external experts to assess cyber crime vulnerability, and quantify it.** To comply with corporate governance best practices, an organization should hire a third-party expert to evaluate the organization’s cyber risk and the potential financial impact of a breach. It is often difficult for employees who have designed systems or who work with them everyday to be critical enough to spot issues of concern. Test the system from the inside
and the outside to determine vulnerability for hacking or other ways to breach the system. Conduct these external audits annually or more often if new technology is being introduced to the organization.

5. **Consider risk transfer solutions.** Now is the time to consider an insurance solution for cyber exposure. Because security breaches typically occur in areas of the organization generally considered to have adequate security protocols — or in unanticipated areas — insurance makes good sense. There are many products now available that take into consideration the unique cyber liability risks associated with the healthcare industry. While there is no replacement for sound risk management practices, a comprehensive insurance policy can be a solid last line of defense.

6. **Involve the Human Resources team.** Internet security must be part of organizational processes at every level and in all parts of the business. As the driver of company culture, HR can help support and strengthen information security campaigns and procedures. Because the lines between employees’ personal conduct and their business conduct — during business hours — can sometimes become blurred, HR, along with the compliance and legal departments, must clearly define and communicate the company’s privacy policy, as well as all rules and requirements regarding employees’ use of the Internet. In addition, HR should continuously monitor employees’ use of social networking sites and remind employees the Internet is a public forum.

The number of data security breaches within healthcare organizations continues to grow and, as healthcare providers and organizations rely more heavily on technology and the Internet to facilitate communication, it is likely that cyber liability will remain a significant business risk in need of vigilant management. Every healthcare provider and organization must be aware of these risks, their role in minimizing it and work collaboratively to protect the privacy and security of the patients under their care. At the same time, they must be aware of how these technologies, when used appropriately, can help the provider achieve safer, more coordinated, efficient and effective care.

**References**


v Ibid


ix http://www.brunswickcompanies.com/pl-cyberliability-insurance.html
Disclaimer

This article is intended for informational purposes only. It is not a guarantee of coverage and should not be used as a substitute for an individualized assessment of one’s need for insurance or alternative risk services. Nor should it be relied upon as legal advice, which should only be rendered by a competent attorney familiar with the facts and circumstances of a particular matter.

© 2011 Beecher Carlson Insurance Services, LLC. All Rights Reserved.

About The Author

Barbara J. Youngberg has joined Beecher Carlson as a Consultant to the national healthcare practice. She has over 25 years of experience in the healthcare industry focused on legal and regulatory issues, risk management and patient safety concerns and internal operations in academic medical centers and complex teaching hospitals. Barbara currently works as a Visiting Professor and Director Faculty of the On Line Programs at the Beazley Institute for Health Law and Policy at the Loyola University College of Law in Chicago. Contact Barbara Youngberg at barbara.youngberg@gmail.com.