UHY LLP Certified Public Accountants

HEALTH CARE INSIDER

VOLUME 7 :: ISSUE 4

In This Issue:

CMS ISSUES FINAL RULE ON EMERGENCY PREPAREDNESS

In response to a number of disasters in recent years (terrorist attacks, hurricanes, flooding, etc.) The Center for Medicaid and Medicaid Services (CMS) has published its final rule on Emergency Preparedness requirements. CMS believes the final rule will increase patient safety during emergencies and ensure a more coordinated response to man-made and natural disasters.

Virtually all health care providers participating in the Medicare and Medicaid programs will be required to meet four common best practices standards. Health care providers include hospitals, long term care facilities, hospices, ambulatory surgery centers, federally qualified health centers and many other health care providers and suppliers. Refer to the actual rule for a list of all entities affected.

The four best practices standards are as follows:

Risk Assessment And Emergency Planning

Facilities have to perform a risk assessment using an "all-hazards" approach that will be the basis for their emergency plan. The risk assessment will be used to identify essential components to be incorporated into the facility's emergency plan. It is expected that the risk assessment will consider (1) all business functions essential to operations that should continue during an emergency, (2) all risks the entity may reasonably expect to confront, (3) all contingencies to plan for, (4) consideration of the entity's location, (5) the extent to which operations may cease or be limited, and (6) what arrangements with other health care entities may be needed to ensure essential services could be provided during an emergency.

Policies And Procedures

Based on the risk assessment, policies and procedures should be developed and implemented that support the successful execution of the emergency plan. Items covered include addressing the provision of subsistence needs for staff and patients, the provision of

Continued on Page 2...

VIRTUALLY ALL HEALTH CARE PROVIDERS PARTICIPATING IN THE MEDICARE AND MEDICAID PROGRAMS WILL BE REQUIRED TO MEET FOUR COMMON BEST PRACTICES STANDARDS.

Continued from Page 1...

alternate sources of energy to maintain safe and sanitary storage of provisions, emergency lighting, fire detection and alarm systems, among other requirements.

Communication Plan

Facilities are required to develop and maintain an emergency preparedness communication plan that complies with federal and state law. Patient care must be well coordinated not only within the facility, but also with other health care providers, state and local health departments and emergency management agencies. In an emergency situation, it is critical to have a system to contact staff, physicians and other necessary people in a timely manner to ensure that the continuation of patient care is carried out in a safe and effective manner.

Training And Testing

Requires each facility to develop and maintain an emergency preparedness training and testing program, which would include initial and annual training for new and existing staff. The facility should conduct drills and exercises to test the emergency plan to identify gaps and areas needing improvement.

It should be noted that not all requirements apply to all types of health care providers. For example, the requirement to have emergency and stand-by power systems is only required for hospitals, critical access hospitals and long term care providers. Thus the rule has been adjusted to reflect the different characteristics of each type of health care provider or supplier.

Since health needs do not stop when disasters strike, CMS believes all parts of the health care delivery system need to be able to continue to provide care. In fact, needs often increase during disasters. And disaster preparedness is not just the responsibility of hospitals, but of many other providers.

The rule contains a number of helpful reports, tool kits and samples. The final rule was published in the Federal Register on Sept. 16, 2016 and goes into effect 60 days later. Health care providers and suppliers must comply and implement these regulations one year after the effective date. We encourage you to read the final rule to determine how your institution may be affected.

By Richard M. Lipman, CPA
National Health Care Practice Leader

> “Since health needs do not stop when disasters strike, CMS believes all parts of the health care delivery system need to be able to continue to provide care.”

THE NEW REALITY: YOUR COMPANY'S DATA BREACH IS INEVITABLE

IT security is a growing threat for businesses of every type, and for health care companies, a data breach has its own particular grave set of ramifications. Health care is among the industries being hit hardest in cyberattacks.

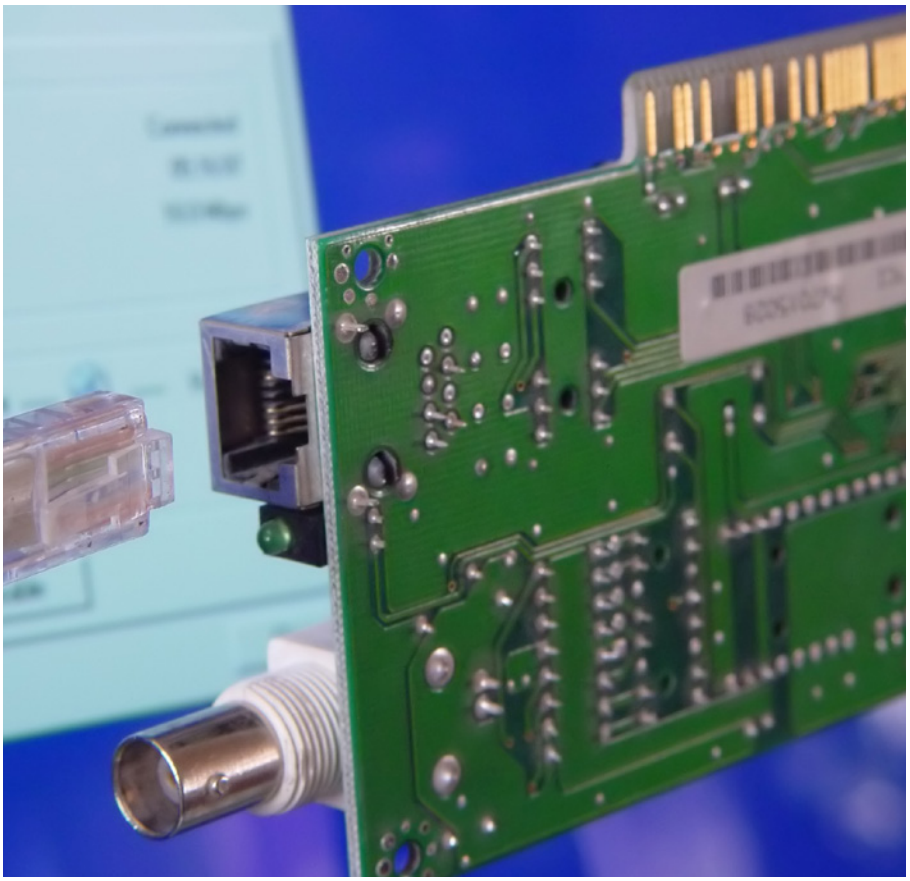
In May, hackers locked data files at Kansas Heart Hospital in a ransomware attack. The hospital paid the ransom, but the attackers didn't fully unlock the files and demanded additional payments before unlocking them. Health insurer Anthem's huge data breach in February 2015 exposed information from 78 million people. And those are just two examples from hundreds to choose from.

Some additional facts to ponder:

- Nearly 90% of all health care organizations suffered at least one data breach in the past two years, which can cost millions per hack.
- According to the newly released Sixth Annual Benchmark Study on Privacy & Security of Health care Data by the Ponemon Institute, data breaches cost the health care industry some $6.2 billion. Further, about 79% of health care organizations say they were hit with two or more data breaches in the past two years.
- 87% of health law attorneys think their clients are at a greater risk of cybersecurity attacks than other industries, according to a survey released earlier this year.

The risks are growing, and health care is vulnerable.

Aside from direct costs, the indirect costs associated with data breaches are rising. This year more customers are abandoning their relationship with companies after they experience a data breach. Industries with the highest turnover are health, pharmaceuticals and financial services. These short and long-term costs are consequences a health care company cannot afford to endure.



While compliance and regulatory laws have helped, more needs to be done to prevent the loss of data through cybersecurity attacks, negligence or technological failure.

Since the federal government started requiring the reporting of health care data breaches, the U.S. Department of Health & Human Services has tracked major health care incidents (those affecting 500 people or more), and the number of people who have compromised health data now exceeds 120 million. Despite HIPAA, Sarbanes-Oxley and other compliance regulations to keep information protected and accurate, the true responsibility of IT security falls on the shoulders of each organization.

WHO AND WHAT IS AT RISK?

A data breach most commonly entails the compromise of valuable information, and each company defines that value differently. In the health care industry, it is confidential patient medical records and personal information.

Hackers today have become savvier, learning new ways to infiltrate networks, including utilizing social engineering and email phishing to obtain valid IDs and passwords from authorized users. As technology has advanced to increase protection, cyber criminals have learned to prey on the weakest security link: people.

Employees have ready access to company information and are often ignorant about how to detect and prevent breaches because of a general lack of training. That means a cyberattack at your company is no longer a question of if, but when.

Continued on Page 5...

Continued from Page 4...

PREPARING FOR A DATA SECURITY BREACH

The starting point in planning for cyberattacks is implementing an incident response plan (IRP) to ensure appropriate action if security is breached. An effective IRP will address preventative controls, timely detection of potential problems and rapid response to data security breaches.

The key components of a well-defined IRP include:

- **Incident response team** – Select individuals from departments that will be involved when a data security breach occurs, such as executive management, information technology, compliance, human resources, public relations, legal, and operations. Identify the roles each incident response team member will play and ensure they have the authority to execute.

- **Data classification** – The organization's incident response strategy takes into account the type of data compromised by the breach in determining its response efforts and activities. Categorize data so employees know how to handle various types of information. Levels can include "public/non-classified," "internal use only" and "confidential." Then, focus on protecting the most confidential data first.

- **Communication plan** – A comprehensive communication plan involves more than maintaining a current contact list of incident response team members, system support personnel and external service providers. The organization should also plan what message it wants to convey and to whom it will communicate internally and externally after a security breach. Include an alternative plan when the normal notification process is pre-empted.

- **Training** – Incident preparedness training ensures that all company personnel are ready to handle data breaches before they occur. Incident response team members should be well versed in how to appropriately evaluate, respond and manage security incidents. Even if not directly involved in the incident management process, all staff should understand the company's overall breach response plan so that their actions support, not hinder, breach response efforts. The Cost of Data Breach Study reports that board involvement reduces the cost of each data breach by $5.50.

- **New threats** – It is critical that health care companies are aware of the new risks and new ways to address them, allocating time regularly to exploring new threats and new controls.

- **Testing** – The IRP should be thoroughly and continuously tested in advance of an actual data breach to help identify process gaps and provide assurance that the plan will be effective in responding to incidents.

All it takes is one person clicking through on one malicious email link to endanger the security of an entire organization and its data. When doctors, nurses, lab technicians or any member of the staff lose a company laptop, input improper credentials or fail to work on a secure network, a company's IT security is compromised. Without a doubt, employees are the weakest link in the security chain. Cyber criminals not only understand this, but exploit it.

The average cost of data breaches today can be significant. Your company must manage this risk. Even though companies may properly prepare, data breaches will continue to happen. We will always be vulnerable, but how we prepare can help ease the pain when an attack hits.

By David Barton, Managing Director at UHY Advisors and leader of the firm's Internal Audit, Risk and Compliance practice. Barton specializes in information security and technology risk and controls.

PROVIDING VALUE TO THE HEALTH CARE INDUSTRY

Today's growing and advanced health care industry is a fast-paced environment where regulatory issues, competition, and rapidly changing consumer expectations converge. Managing risks and realizing opportunities becomes a more important focus as health care organizations decide how they will adapt and evolve their business models for long-term survival.

Ensuring today's actions will lead to achieving long-term goals can be a major challenge for anyone. Many health care organizations are unable to address the issues at hand and consider the "big picture" because they are overwhelmed with urgent matters and patient care. UHY LLP's National Health Care Practice brings an understanding of the industry together with innovative solutions that have a positive impact on bottom line. We understand the challenges facing health care providers and facilities.

OUR LOCATIONS

CA Irvine 949 556 8905
CT Norwalk 203 401 2101
CT West Hartford 860 519 1726
GA Atlanta 678 602 4470
MD Columbia 410 423 4800
MD Frederick 301 695 1040
MI Detroit 313 964 1040
MI Farmington Hills 248 355 1040
MI Sterling Heights 586 254 1040
MO St. Louis 314 615 1301
NY Albany 518 449 3171
NY New York 212 381 4800
NY Rye Brook 914 697 4966

ADDITIONAL UHY ADVISORS LOCATIONS

IL Chicago 312 578 9600