UHY LLP
Certified Public Accountants

HEALTH CARE INSIDER

VOLUME 5 :: ISSUE 3

In This Issue:

Medicaid Managed Care Continues To Expand Across The US

Traditionally, medical services payments for patients covered by Medicaid have been through the fee-for-service system. Since close to 30 states have or are planning to implement managed care payment systems for Medicaid enrollees, the days of Medicaid fee-for-service payments are coming to an end. Approximately 50 million people currently receive Medicaid benefits through some form of managed care. Most are children and adults under age 65. But as managed care continues to expand, expect that elderly beneficiaries will be expected (or required) to sign up for managed care programs. Depending on the state, Medicaid managed care may be voluntary or mandatory.

In a managed care environment, the managed care organization (MCO) pays for benefits provided to its enrollees in exchange for a monthly payment from the state. The MCO contracts with various medical providers to care for its enrollees. The "cost risk" is transferred from the state to the MCO. No longer will providers be paid by the State. Some states have made contracting easier by setting the managed care Medicaid rates so providers do not have to negotiate with the MCOs. Other states are encouraging the negotiation process.

Continued on Page 3...

APPROXIMATELY 50 MILLION PEOPLE CURRENTLY RECEIVE MEDICAID BENEFITS THROUGH SOME FORM OF MANAGED CARE.

Continued from Page 1...

The overriding reasons for the changes are cost savings and moving patients into the lowest level of care as quickly as possible. A side benefit is downsizing of government. But don't expect the shift to managed care to produce savings in the short term. Long term savings may be achieved by improving care management and health outcomes.

The MCOs will drive how the providers are paid, how often and how many referrals the provider receives and how long the patient will stay in the facility. Medicaid managed care will not affect how facilities care for their patients but is likely to affect demographics and length of stay. Expect shifts to less acute, less institutional settings, including assisted living and home care. Expect to see patients with higher acuity in assisted living facilities.

MCOs will have measures to assess the quality of care, so providers should be aware of what is being measured. The MCO may have an interest in quality but is likely more focused on outcomes. Since one of the goals of MCOs is to keep patients in hospital and skilled nursing facility beds for as few days as possible, maintaining census will present new challenges for facilities, especially those with high Medicaid populations. Thus, providers need to make sure the MCOs see them as worthy of referrals to keep up the stream of new admissions.

In addition, providers may have to start or grow post-acute services, and consider ways to diversify. Providers can no longer afford to be a one-of-a-kind service provider. For example, skilled nursing facilities may want to look at providing adult day care, assisted living, respite care, hospice care or other options. MCOs likely will seek out providers who offer a variety of services and can quickly move patients seamlessly from one care setting to another.

Providers will also need to manage cash flow. It seems as if states new to the Medicaid managed care bandwagon experience more delays and glitches in the payment scheme. Make sure you invest in staff training and provide the necessary support to work with the Medicaid MCOs. You should establish eligibility for Medicaid managed care as soon as possible to avoid unnecessary delays in getting payments approved. Take care in how you bill the MCO. Some states have established rules regarding timely payments of "clean" claims. Understand what information and in what format a "clean" claim must be to avoid delays in payment. Specialty services such as long-term ventilators may require extra paperwork.

Before contracting with a managed care provider, do your homework. Some things to consider include knowing what it costs to provide the services you are expected to provide, whether the MCO you are contracting with is financially stable, and how your facility's performance compares to other facilities in your area. Engage professionals who are prepared to assist you with cost finding and accounting, pricing and negotiation, cost of establishing new services, etc.

By Richard M. Lipman, CPA
Health Care Practice Partner

Health Care Cyber Threats And Data Security

Data breaches are in the headlines almost every day announcing that some large company has failed to secure their customer data. It is only a matter of time before health care data breaches start to eclipse the payment card breaches. In a recent article published by Reuters, the FBI stated that the health care sector is vulnerable to cyber attacks and that health care data is even more profitable than even credit card data.

Risk factors

Changes in the medical information technology environment along with more compliance regulations have created a situation where personal health information is more vulnerable than ever before. The push to digitize data so it is shared among health care providers has increased the risk of compromise dramatically.

Another contributing factor is that more electronic devices are now storing and transmitting health care data over the internet. These devices can pose a significant threat if they are not configured properly. Complicating things even more is the culture of BYOD (Bring Your Own Device) which could commingle personal and patient data. These devices need to be properly configured and secured to prevent unauthorized access to that patient data.

Risk assessment

The HIPAA Security Rule requires that all organizations that create, receive, maintain and transmit ePHI (electronic protected health information) evaluate risks and vulnerabilities in their environments and implement reasonable security measures to protect that information. The first step of the risk assessment is to identify all the devices connected to the network. The next step is to ensure that these devices are properly configured and that access is limited to authorized individuals. An inventory of these devices should be maintained with periodic reviews to ensure that no unauthorized access points have popped up on the network.

The next step would be to take an inventory of where all the electronic health care data resides so that it can be secured and monitored along with other sensitive data. Be sure to include backup data and the location of the backup data in that inventory. Determine the individuals (employees, patients and third parties) who have access to that ePHI and decide if it is appropriate for their job responsibilities and duties.

Threats

When organizations identify the various threats to ePHI, Malware is the first and most popular that is listed. However, according to Ponemon Institute's Fourth Annual Benchmark Study on Patient Privacy & Data Security, the number one reason for an incident is due to a lost or stolen computing device. The number two reason for an incident is due to unintentional employee action. These surveys and other studies over the past four years seem to point to employees as being the weakest link in maintaining the security of health care data.

Malware is a constant threat to any type of sensitive or confidential data along with Advanced Persistent Threats commonly referred to as "APT". APTs consistent of groups, businesses or governmental agencies which utilize malware to exploit vulnerabilities for various motives. The motive with health care data as mentioned previously is that it is highly profitable. That data can be billing records, medical files, payment details etc.

Social engineering is another threat that utilizes weaknesses in employees to gain unauthorized access to information or resources. Employees should be properly trained to not give out any information that is not first approved by management.

Continued on Page 5...

> "Data breaches are in the headlines almost every day announcing that some large company has failed to secure their customer data."

Continued from Page 4...

Practices to reduce risk of data breach

It should be mentioned that following good security practices and being in compliance with regulations does not guarantee that the organization will not suffer a breach. It will however reduce the risk of a breach and help to reduce any fines and penalties in the event of a breach if it is ascertained that the organization was in compliance and followed reasonable and sufficient security procedures.

Best practices to have in place to help prevent and/or detect a breach timely include:

- Strong security policy with robust password requirements
- Periodic reviews of access rights
- Inventory of devices and data to identify scope of environment
- Knowledgeable individuals with proper expertise to secure that environment
- Monitor network activity and perform periodic vulnerability scans
- Annual audit or assessment by third party to determine security status of environment

Recent surveys of health care data, including Ponemon's benchmarking study mentioned above, indicate the largest weakness and cause of data breaches are employees. Having said that, one of the most important and cost effective methods of reducing risk is by making your employees aware of the risks and training them on how to avoid and detect any abnormalities that may occur.

It is no surprise with the requirement of health care data to become digitized and to become available over the internet that the risks of unauthorized breaches would increase accordingly. While recently the number of breaches has fallen it is only a matter of time before that the number climbs back up. The volume of data being shared on health information exchanges will increase along with more devices being connected to the internet and networks of health care organizations.

Organizations need to make sure that they are in compliance with various regulations and have an adequate set of policies and procedures in place to be reasonably assured that protected health information is secure. They also need to be sure that their business partners maintain proper security policies and are also in compliance with regulations. An annual risk assessment along with an annual assessment of security controls are critical to maintaining that the environment is reasonably secured and in compliance with regulations.

By Jeffrey Streif, Principal
National Health Care Practice

Jeffrey is a CPA, CISA, CFE and QSA. He is a leader of the firm's National Management and Technology Consulting Practice and a Certified Common Security Practitioner for HITRUST. Jeffrey is the former Chair of the MSCPA Information Technology Committee and current Board Member of the St. Louis Chapter of ISACA. He was recently named to the AICPA's Cyber Security Task Force.

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

CT	New Haven 203 401 2101
GA	Atlanta 678 602 4470
MD	Columbia 410 423 4800
MI	Farmington Hills 248 355 1040
MI	Sterling Heights 586 254 1040
MO	St. Louis 314 615 1301
NJ	Oakland 201 644 2767
NY	Albany 518 449 3171
NY	New York 212 381 4800
NY	Rye Brook 914 697 4966
TX	Dallas 214 243 2900
TX	Houston 713 561 6500

ADDITIONAL UHY ADVISORS LOCATIONS

IL	Chicago 312 578 9600
DC	Washington 202 609 6100

Our firm provides the information in this newsletter as tax information and general business or economic information or analysis for educational purposes, and none of the information contained herein is intended to serve as a solicitation of any service or product. This information does not constitute the provision of legal advice, tax advice, accounting services, investment advice, or professional consulting of any kind. The information provided herein should not be used as a substitute for consultation with professional tax, accounting, legal, or other competent advisors. Before making any decision or taking any action, you should consult a professional advisor who has been provided with all pertinent facts relevant to your particular situation. Tax articles in this newsletter are not intended to be used, and cannot be used by any taxpayer, for the purpose of avoiding accuracy-related penalties that may be imposed on the taxpayer. The information is provided "as is," with no assurance or guarantee of completeness, accuracy, or timeliness of the information, and without warranty of any kind, express or implied, including but not limited to warranties of performance, merchantability, and fitness for a particular purpose.

UHY LLP is a licensed independent CPA firm that performs attest services in an alternative practice structure with UHY Advisors, Inc. and its subsidiary entities. UHY Advisors, Inc. provides tax and business consulting services through wholly owned subsidiary entities that operate under the name of "UHY Advisors." UHY Advisors, Inc. and its subsidiary entities are not licensed CPA firms. UHY LLP and UHY Advisors, Inc. are U.S. members of Urbach Hacker Young International Limited, a UK company, and form part of the international UHY network of legally independent accounting and consulting firms. "UHY" is the brand name for the UHY international network. Any services described herein are provided by UHY LLP and/or UHY Advisors (as the case may be) and not by UHY or any other member firm of UHY. Neither UHY nor any member of UHY has any liability for services provided by other members.

www.uhy-us.com