In recent years, the health care industry has become susceptible to cyberattacks and lags behind other industries when it comes to cybersecurity. The shift from paper records to electronic records has left the industry with a difficult challenge: improving patient experience with online charts and quick turnaround of results, while simultaneously protecting all patient information. In order to understand the magnitude of the risk of insecure patient records, health care providers need to recall the vulnerable information they retain from patients, including social security numbers and credit card information. Due to the vast amount of valuable information available, it is no surprise that when broken down by industry, health care was the second-most attacked industry. Cyber breaches alone cost the health care sector $6.2 billion each year. For most industries, negative financial consequences is the worst case scenario. In the healthcare industry, however, there is much more at stake: a patient's health.

What's the prognosis?
On the brink of a cyberattack, concern is quickly focused on the patient. There is little argument that this is exponentially important, but the long-term financial consequences must also be considered. For example, a ransomware attack could cause health care providers to jump to the first solution without considering the lasting effects. Ransomware is a form of malware in which your access to systems or data is held hostage until a “ransom” is paid. In 2018, almost half of the ransomware incidents reported involved health care companies. Ransomware attacks are practically dangerous for the health care industry since loss of control of systems or loss of access to data can put a patient’s life at risk. If the ransom is paid in order to regain control of software systems, the financial consequences can have a lasting effect.

Following any form of data breach, health care professionals are likely to be distracted from patient care and funds that could be used towards patient care

Continued on Page 2...
THE HEALTH CARE INDUSTRY IS VERY SUSCEPTIBLE TO CYBERATTACKS AND THE AFTERMATH COULD BE DETRIMENTAL.
may have to be used to restore systems. The average health care organization had to spend $1.4 million to recover from a cyberattack. In order to fix some of the damage to public image following a security breach, a health care system may have to spend almost three times more on advertising than it would normally spend, adding another financial burden.

In addition to the financial consequences, the intangible consequences must also be considered. According to a study, 54 percent of patients said they would be likely to change providers after a security breach. Since health care runs on trust, it is critical that providers are able to maintain the trust of their patients. Patients are more likely to limit communication with their doctors if they feel they cannot trust that their information is secure, and without a full picture from a patient, providers are restricted in their ability to treat patients. Data suggests that more than 2,100 patient deaths annually could be attributed to hospital data breaches. Researchers explained that a data breach both diverts funds from patient care and distracts physicians for years after the attack.

Prevention is key
The health care industry is very susceptible to cyberattacks and the aftermath could be detrimental. Follow these tips to prevent a cyberattack:

- Take the time to identify potential inefficiencies in cybersecurity. The US National Institute of Standards and Technology offers guidance on assessment and improvement in an organization’s ability to prevent, detect, and respond to cyberattacks. The five key functions outlined in the framework are (1) identify, (2) protect, (3) detect, (4) respond, and (5) recover.
- Ensure employees are properly trained: Human error is the leading cause of data breaches today. Employers need to educate employees on the basics of cybersecurity. Additionally, employees need to be informed that cybersecurity is the responsibility of all employees. If employees are trained to spot suspicious communications (such as phishing emails) and are able to report it to IT in a timely manner, the threat can be diverted before it is too late. Employee training programs also help create a culture that is focused on security.
- Limit access: Access to information should only be granted to those that need to use or view the data. Physical access should be controlled as well. Computers and other electronics that contain protected information should be physically locked to an area.
- Make sure systems are regularly backed up and that the backups are secured and easily accessible.

Taking immediate action when faced with a cyberattack is the first step to recovery. The more prepared an organization is, the sooner it will be able to identify and respond to an incident. UHY Advisors has an experienced cybersecurity team to arm your employees and your practice against cyber attacks. Contact us in one of our many locations before valuable information is lost and lives are at stake.

By Krysten Backhus
Staff Accountant

Sources:
https://phoenixnap.com/blog/ransomware-statistics-facts
MGMA Article
Health care is not only one of the largest industries, but it is also one of the most complex. The combination of the size and complexity of the industry has resulted in endless frustration for practice managers when interpreting intense quantities of data. How are industry leaders supposed to make sense of this convoluted information and turn it into stronger results? The answer, in short, is benchmarking. Benchmarking, in this instance, is comparing the processes and metrics of a single business to those in the industry.

In order to effectively benchmark, practice managers must first make sure they are utilizing useful, reliable, and up-to-date information. This starts with being able to rely confidently on your internal data, typically a practice’s electronic health care record (EHR) and accounting systems. For external data, practice managers should conduct due diligence and identify an external source they can extract quality benchmarking data from. There is an extensive list of consulting firms and technology companies covering the health care space, such as the Medical Group Management Association (MGMA), that provide relevant information, as well as insight on benchmarking data.

Once comfortable with the sources of data, the next step is to understand the business objectives of the practice and to select benchmarks that can best identify what is necessary to improve performance. It should also be noted that it is critical to consider the unique aspects of each practice (i.e. specialty, size, and market forces) during the selection of benchmarks. This will allow for the identification of benchmarks that add real value to a practice. As it pertains to health care some of the most frequently used metrics include: operating costs per procedure or per visit, operating costs as a percentage of revenue, collections per provider, visits per day, and days in accounts receivable.

Another consideration is what form of benchmarking to use. Benchmarking at its base has two different approaches: internal and external.

1) **Internal benchmarking** involves the analysis of two departments within the same practice. When one department outperforms another, this information can be dissected to enable better processes to be implemented throughout the organization. It should be noted that all benchmarking should begin with internal benchmarking as it requires the organization to examine its own performance and creates a baseline for other benchmarking strategies.

2) **External benchmarking** is the comparison of performance to industry leaders in order to obtain new ideas and methods to improve. This should be done continuously to analyze how industry leaders achieve success. External benchmarking involves three alternatives: competitive benchmarking, functional benchmarking, and generic benchmarking.

a) **Competitive benchmarking** is the comparison of performance to direct competitors only. This type of benchmarking is difficult as it can be challenging to obtain the necessary data. Despite the difficulty of obtaining the required information this method should be attempted as it allows a practice to stay in tune with its external environment and helps ensure a continuous focus on improvement.

b) **Functional benchmarking** is the comparison to successful businesses performing the same or similar functions, but operating outside of the immediate industry. For example a doctor’s private practice could be benchmarked against another professional service provider such as a lawyer or accountant.

c) **Generic benchmarking** takes a broader look at results comparing performance based on business functions regardless of industry. An example of this strategy would be comparing the performance of a hospital’s accounting department to the accounting department of a construction company. This method of benchmarking can be executed without as much difficulty as competitive benchmarking, as organizations operating in different industries may be more willing to share their data. Note that this data will need modifications to be comparable in a beneficial manner to the company’s own metrics.

Proper implementation of benchmarking will allow practice managers to not only understand what is influencing their practice’s current level of performance, but also develop a sound strategy to improve it. As the health care industry continues to expand, it will become more important for industry members to analyze their own data, which will be useless unless they can develop an understanding of what they are looking at.

By Norm Bird
Staff Accountant

Sources:
http://www.fmshk.org/database/articles/06nbdrilkay.pdf
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3359088/
https://www.oshatrain.org/notes/2fnotes04.html

SALES AND STRATEGIC PARTNERSHIPS OF YOUR MEDICAL PRACTICE: 10 FINANCIAL CONSIDERATIONS

The “Amazon effect” is finally being felt in healthcare. With this phenomenon, more emphasis is placed on data, which means more money on technology and systems, and bigger investments in infrastructure. Not every practice will have the resources to manage this seismic disruption, and those that fail to keep up may find themselves at a competitive disadvantage. More than 500 hospitals have merged into larger health systems in the past 10 years. In the last six years, $100 billion has been spent on hospital consolidation. Thinking about a sale or strategic partnership? Below are 10 factors to consider:

**Taxes**
When structuring a transaction, maximizing tax efficiency while meeting the legal and tax structuring requirements of the buyer/investor is paramount. Normally, the purchase price is paid at closing and, if structured properly, the majority of proceeds can potentially be treated as long-term capital gains which are taxed lower than ordinary income. This is especially important in states with higher state and local taxes, which are capped at $10,000.

**Accounts receivable**
Are accounts receivable factored into the valuation? Does the buyer or seller get the accounts receivable and other working capital assets and liabilities? There are sizeable tax ramifications as it relates to accounts receivable.

**Method of accounting**
Method of accounting can make a difference in how earnings are calculated, impacting the valuation. Consider revenue timing and capital expenditures, especially since cash basis accounting is prevalent in the industry.

**Value**
How much is your practice worth? The payment received is generally reflective of expected earnings over time. That figure is then given a multiple — x times earnings — to arrive at a practice value. Several factors make up that multiple: type/scope of practice, rate of revenue/industry growth, and needs of the investor. Deals may be structured with incentives and milestones (earn-outs) included.

**Payment**
Payment received may come in many forms such as: cash, rollover stock, ongoing profit participation and earn-outs. As a deal may include a mix of all of the above, it is important to consider how these factors change the value of the transaction and what income is guaranteed and what income and potential tax liability is deferred.

**Sharing the proceeds from the sale**
In some practices there may be non-owners that have been instrumental in the success of the practice or that have been with you for many years that you want to reward in the event of a sale. The terms of these types of arrangements should be agreed upon up front as part of the negotiations with the investor/buyer.

**Real estate**
Do you own any real estate? Will the real estate be included in the transaction?

**Synergies**
How do you make sure you are making the most of post-closing value? Does the buyer have plans to invest in the practice? Is there potential to increase revenues through investment in ancillaries or with add-ons and new office openings?

**Malpractice**
Potential tail insurance costs need to be taken into consideration, this often requires a conversion from a claims-made policy to an occurrence policy. Both parties need to agree upon who will bear the cost of the insurance policy.

**Post-closing obligations**
Sellers need to be aware of clinical and practice leadership responsibilities that may be required after the deal is closed.

For more information, contact your healthcare professional in one of our many locations.

Sources:
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 949 623 8803
CT  Farmington 860 676 9020
FL  Miami 305 438 7993
GA  Atlanta 678 602 4470
MD  Columbia 410 423 4800
MI  Ann Arbor 734 213 1040
MI  Detroit 313 964 1040
MI  Farmington Hills 248 355 1040
MI  Sterling Heights 586 254 1040
MO  Kansas City 816 741 7882
MO  St. Louis 314 615 1301
NY  Albany 518 449 3171
NY  New York 212 381 4800
NY  Saratoga Springs 518 583 1234
NY  Rye Brook 914 697 4966
TX  Houston 713 325 7870

Additional UHY Advisors Locations

IL  Chicago 312 416 4150

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 UHY 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 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.

©2019 UHY LLP. All rights reserved. [0519]