Ann & Robert H. Lurie
Children's Hospital of Chicago™
Children's Community Physicians Association

TABLE OF CONTENTS:

ccpa news

SUMMER/FALL 2015

Letter from CCPA's Executive Director Kena Norris, MJ, FACHE

Much like the healthcare industry, how quickly do the seasons change in the Chicagoland area as fall is already upon us. And as we head into cooler temperatures, there have been a few changes at Children's Community Physicians Association (CCPA) that I am pleased to share.

First, the CCPA election resulted in two new board members – Dr. Douglas Ashley from Lake Forest Pediatric Associates and Dr. Ushma Patel from ABC Pediatrics, LTD. While we were sad to see Dr. Daniel Lum and Dr. Aleta Clark leave the CCPA board after so many years of dedicated service, we are also excited about the contributions from our newest board members.

In addition, the CCPA board elected its officers to the executive committee - Dr. Dov Shapiro, President, Associated Pediatric Partners, SC; Dr. Valerie Kimball, Vice-President, Traismans, Benuck, Merens & Kimball; and Dr. Michael Siegel, Treasurer/Secretary, PediaTrust Highland Park Pediatric Associates. We look forward to their leadership as CCPA continues its transition with Lurie Children's Health Partners Clinically Integrated Network.

I would like to thank everyone who attended the 2015 CCPA Annual Meeting, which had record attendance. We also appreciate the numerous practices that reached out to staff to commend American Academy of Pediatrics' Board of Director, Dr. Richard Tuck, for his insightful presentations and some members even requested that CCPA bring him back as a speaker again next year. As members, your opinions matter so that we can continue to make the annual meeting an event you look forward to attending.

Another exciting change this summer was the launch of a new, user-friendly CCPA website, which can be found

continued from page 1

at **www.ccpaipa.org**. Aside from its modern design, you will now find several resources that are for members only, including the newest CCPA benefits (American Academy of Pediatrics' Red Book Online and ICD-10 Newsletter), in the members' portal section. Other features of the new website include its mobile friendly design, the ability to readily pay annual dues, register for upcoming events, and view the latest association updates online in real time. As we further develop our member communications, we hope to make the CCPA website a one-stop-shop for your membership needs.

Finally, as the executive director of CCPA Purchasing Partners (CCPAPP) too, I am pleased to report that our group purchasing membership grew this year by nearly three times the average annual growth than in prior years. And as most of you are already aware, the bulk of CCPA's revenue is generated by its group purchasing. Subsequently, CCPAPP's substantial growth should result in increased revenue for CCPA, which can then be used to further develop member services.

This is an exciting and transformational time for CCPA, but we will only make changes that are beneficial for our members. Therefore, please do not hesitate to share your comments, questions, ideas or concerns with the CCPA board and staff as it will only help in our organization's continued evolution. ■

Association Updates

CCPA Staff Update

After years of dedicated service, we are pleased to announce that LaVonna Swilley was recently promoted to CCPA Manager of Operations, but will remain the primary contact for members' managed care and credentialing questions. LaVonna can still be reached at **312.227.7425** or **lswilley@luriechildrens.org**.

CCPA/CIN Transition Update

CCPA is in a partnership with Lurie Children's and the Faculty Practice Plan to create a Clinically Integrated Network (CIN). CCPA is maintaining its seventeen payor contracts, but will slowly start terminating these contracts as the CIN establishes new payor agreements with improved reimbursement for community physicians.

Currently, the CIN has contracts with Blue Cross Blue Shield of Illinois' intensive medical home program, MyCare Chicago (soon to be Molina) and Meridian, but is working on relationships with other payors, including Aetna. For questions about CIN contracts, please contact Scott Wilkerson, Executive Director at **312.227.7320** or **scwilkerson@luriechildrens.org**.

CCPA Purchasing Partners (CCPAPP) Annual Seminar

Register today! Time for a Checkup: Improving the Business Health of Your Practice is set for Thursday, November 19, 2015. The seminar will be held at Café La Cave located at 2777 Mannheim Rd in Des Plaines, IL. For more information, please visit **ccpapp.org/check-up-registration-2015**.

CCPA Member Website

If you have not already, please be sure to check out the new CCPA website at **www.ccpaipa.org**. It contains news, updates and resources that are exclusive to CCPA members, which can be found in the members' portal section. Please contact LaVonna Swilley, CCPA Manager of Operations, at **312.227.7425** or **lswilley@luriechildrens.org** for your practice's login and password information.

CCPA News

Lastly, *CCPA News* has expanded its content to cover pertinent healthcare law, practice management, and other related issues using experts in these areas. If there is a legal, regulatory or practice management matter that you would like us to address in the newsletter, please contact Kena Norris, CCPA/CCPAPP Executive Director, at **312.227.7406** or **knorris@luriechildrens.org**.

The Impact of the Affordable Care Act on Private Practices

By Laura S. Goodman, CPA, CHBC, FGMK, LLC, National Society of Certified Healthcare Business Consultants

It is commonly known as the Affordable Care Act, Obamacare, ACA or, generically, as healthcare reform, but a private physician practice may also refer to the ACA as a double-edged sword. A physician practice is a business and it is governed by the ACA rules like any other business. In addition, a physician practice relies on payments from insurance companies as a significant source of income. Therefore, any benefit reductions related to the ACA could potentially impact its annual revenues.

As a business owner, a physician must keep current with ACA compliance, reporting requirements, and the selection of healthcare coverage for its employees. Businesses, as employers, fall into one of two groups: large employers with over 50 full-time (full time = 30 hours/week) employees or small employers with fewer than 50 full-time employees. Large employers were mandated to comply with the ACA as of January 1, 2015, but large employers with only 50-99 full-time employees were given an extension until January 1, 2016 to comply. Small employers represent the majority of businesses in the United States and thereby are not required to comply with the ACA's health insurance mandate.

Large employers are required to offer traditional employer-sponsored plans by their compliance deadline. Small employers can choose to offer a traditional employer-sponsored plan, offer a plan through a Small-Business Health Options Program ("SHOP"), or not offer any health insurance plan at all. However, all individuals in the United States are now required to have health insurance. Employees will need to buy individual health insurance plans, either through the general commercial market or through a government-sponsored health insurance exchange.

Increased Benefit Costs for Employers

The overall cost of health insurance has been increasing on an annual basis and many health insurance industry experts are estimating that premiums could increase by 30-40% over the next two years. This increase would directly impact the bottom line for physician practices that offer health insurance to its employees.

While it is true that small employers can choose not to offer health insurance, the rules related to subsidizing

continued on page 4

continued from page 3

the cost of health insurance for employees are now more stringent. If an employer chooses to reimburse an employee for the cost of an individual health insurance policy, the amount of reimbursement must be added to the gross income on the employee's W-2 wages and cannot be specifically earmarked as a health insurance reimbursement. It needs to be, simply, additional salary. The employer penalty for non-reporting (or incorrect reporting) is $100 per day, per instance.

> Discounted or free wellness check-ups and gym memberships are other value-added employee benefits that can be offered at low cost to the physician practice.

Although the ACA does not mandate employer-provided health insurance plans for small employers, physician practices need to ensure that they maintain good employee morale should they determine that the cost of an employer-sponsored health insurance plan is too expensive. Small employers should consider offering alternative employee-funded pre-tax benefits such as health savings accounts or flexible spending accounts, which have relatively low costs of administration. Discounted or free wellness check-ups and gym memberships are other value-added employee benefits that can be offered at low cost to the physician practice.

Based on current projections, the ACA will most likely increase the cost of employer-sponsored health insurance, change the reporting requirements related to benefits, and potentially have physician practices scrambling to retain good employees should they choose to discontinue offering an employer-sponsored plan. But now let's take a look at the other edge of the ACA sword – the possible impact on physician practice revenue.

Potential Risk of Reduced Revenues

Many health plans offered to individuals in today's market (through commercial brokers or government exchanges) have very high deductibles, high co-pays, and high co-insurance. The resulting phenomenon is that many patients are delaying physician visits until their illnesses are severe. Physician practices are seeing lower volumes, higher acuity, and patient satisfaction is even more critical because patients now perceive a doctor's visit to be a consumer encounter since more of the fees are being paid by the patient instead of the insurance company.

Therefore, physician practices must strategize to maximize their collections. They need to implement procedures to confirm pre-eligibility, collect all co-pays and past-due balances at time of service, and optimize coding. Revenue cycle management becomes critical. The aging of accounts receivable and adjudicated collection rates should be monitored on a regular basis. Rejections and under-payments need to be appealed and the fee schedule should be reviewed at least annually.

Another risk for the physician practice is the fact that individuals who buy insurance on the exchanges have a three-month "grace period." But if the insurance premiums are not paid by the patient at the conclusion of the third month, health plans are only required to pay for claims during the first month of the grace period and can hold the claims for the second and third months. Therefore, the physician practice may be left to pay for medical services provided during months two and three of the grace period if the patient's premium is not paid. This means that not only are physicians potentially facing lower volumes, they may also see an increase in bad debt as it is unlikely that the physician practice will be able to collect those fees from the same patients who did not pay their insurance premiums in the first place.

Given the above, the ACA may become a double-edged sword for private physician practices by raising their overhead costs for employee benefits while increasing the risk of reduced revenues for their medical services. The independent practices that will survive the next decade will be the ones to implement better revenue cycle management procedures and strive to reduce overhead costs, including the cost of benefits, while retaining their key employees. It will not be an easy process, but for many it is worth the effort to maintain control of their own businesses. ■

Are You Hip to HIPAA?

A PEDIATRICIAN'S HIPAA WORKOUT GUIDE FOR COMPLIANCE, STABILITY AND BALANCE [PART II]

By Julie E. Treumann, Esq, de jure de facto, p.c.

Stability, balance and movement are dependent on strong, healthy hip flexors – a key component of today's workout trends. Likewise, the stability of your growing practice depends on a strong healthcare regulatory compliance program. This article provides additional workout tips for your "HIPAA-flexors" to help create, maintain and assess compliance within your practice and to avoid "HIPAA-fractures," which can result in fines, headaches and generalized gluteal pain. Part I of this article covered the Privacy Rule[1]; Part II continues with the Security Rule and Breach Notification Rule.

■ ■ ■

To recap, HIPAA is a collection of rules and regulations enacted as part of the Health Insurance Portability and Accountability Act of 1996, as amended under the American Recovery and Reinvestment Act of 2009 by the Health Information Technology for Economic and Clinical Health Act ("HITECH"). The main components of HIPAA are known as the Privacy Rule, the Security Rule and the Breach Notification Rule (the "Rules").

4. IT Band - Security Rule Summary

Iliotibial (IT) bands can cause lots of pain when weak. For your practice, weak information technology (IT) practices can result in security breaches – also quite painful! In addition to the Privacy Rule, covered entities must also comply with the Security Rule, which lists four standards for safeguarding protected health information (PHI): (i) Administrative Safeguards; (ii) Physical Safeguards; (iii) Technical Safeguards; and (iv) Organizational Requirements.

Administrative Safeguards are your policies, procedures, training and ongoing assessments. These involve security management processes, assigned security responsibility, workforce security, information access management, security awareness and training, security incident procedures, contingency plans, evaluation and business associate agreements.

Physical Safeguards are how you keep records safe in the office space. This includes facility access controls, workstation use, workstation security, and device and media controls.

Technical Safeguards involve how you transmit and receive PHI, such as access control, audit controls, integrity, person or entity authentication and transmission security.

Organizational Requirements include your business associate contracts and other arrangements.

Not every standard in the Security Rule is going to be applicable to each practice; thus, some of the standards are "addressable" meaning that you can address them and determine whether or not implementation is reasonable and appropriate (it does not mean optional) and other standards are "required." The first step to compliance is a security risk analysis and assessment. This can be done internally or with an outside consultant specifically trained in the process and should be documented. As you perform your risk analysis, you should include, at a minimum, the following: (i) evaluate the likelihood and impact of potential risks to e-PHI; (ii)

continued on page 6

continued from page 5

implement appropriate security measures to address the risks identified in the risk analysis; (iii) document the chosen security measures and, where required, the rationale for adopting those measures; and (iv) maintain continuous, reasonable, and appropriate security protections. The Department of Health and Human Services has created a security risk assessment tool that can be used to start and continue your security processes: **www.healthit.gov/providers-professionals/security-risk-assessment-tool**.

> If a breach of unsecured PHI affects fewer than 500 individuals, you need to notify the Secretary of the breach within 60 days of the end of the calendar year in which the breach was discovered.

The most important thing to remember is that security of PHI is not a one-time project, but rather an ongoing, fluid process that will create new challenges and require new policies and procedures as your organization and technologies evolve. If it is one and done, your HIPAA-flexors will become stiff and your policies will become stale. Covered entities should regularly review records to track access to e-PHI and detect security incidents, periodically evaluate the effectiveness of security measures put in place, and regularly reevaluate potential risks to e-PHI. Do not forget often-overlooked places where PHI or e-PHI may be stored, like your copier and fax machines. Be sure to wipe or erase the memory or hard drive before returning or selling these items.

5. Step-Up - Breach Notification Rule

There are times, of course, when there may be a breach of PHI or e-PHI. Most often, this is not because of hackers. Instead, it may result from the loss or theft of a laptop or mobile device, or unauthorized access to medical records. Your policies and procedures should cover training, training and more training as well as disciplinary consequences for breaches, whether intentional or unintentional. Social media use should not be permitted, passwords should be changed often, consider encryption for email and other technology, lock paper files and shred when no longer needed, discuss patients in a closed room and consider noise machines if your treatment room walls are not very soundproof.

Despite your best efforts, when a breach of unsecured PHI does occur, you need to step-up and self-disclose the breach. If a breach of unsecured PHI affects 500 or more individuals, you need to notify the Secretary of the Department of Health and Human Services (the "Secretary") of the breach without "unreasonable delay" and in no case later than 60 calendar days from the discovery of the breach. If a breach of unsecured PHI affects fewer than 500 individuals, you need to notify the Secretary of the breach within 60 days of the end of the calendar year in which the breach was discovered. In addition to notifying the Secretary, you also have to notify the affected individuals, and, in the case of a breach involving more than 500 residents in a state or jurisdiction, to notify prominent media outlets serving the state or jurisdiction.

Keep in mind that of the tens of thousands of cases of breach that the Office of Civil Rights has resolved, by far the most common covered entity that has been required to take corrective action are private practices. Depending on the severity and reason for the breach, as well as corrective actions taken, fines for breach can range from $100 per violation up to a maximum of $1,500,000 in the aggregate.

6. Flexibility - Minors

When it comes to minors, pediatricians need to be aware and understand that the law allows some flexibility. Generally, minors cannot consent to treatment. Rather, the parent, guardian or other person acting in loco parentis must consent to care, and may access the minor's health information. In Illinois, minors are defined as individuals under the age of eighteen.

There are some exceptions under Illinois law when a patient under the age of eighteen may consent to his or her own care, and have the corresponding right to determine access to their health information, if he

There are some exceptions under Illinois law when a patient under the age of eighteen may consent to his or her own care,

or she is: (i) married; (ii) pregnant; (iii) a parent; or (iv) "emancipated" by a formal court proceeding.

In addition, Illinois patients under the age of eighteen may consent to certain treatment as follows:

- Outpatient psychiatry or psychology – parents can only have access to the medical information or the fact that the child is receiving treatment if the child is under twelve or gives consent.
- Treatment and counseling for sexually transmitted disease or human immunodeficiency virus – if the minor is twelve or older, a healthcare provider may tell the parent that treatment is taking place.
- Treatment for alcohol and drug abuse or the effects on a minor of a family member's alcohol or drug abuse – a healthcare provider may not tell the parents without the minor's consent unless it is necessary to protect the minor, a family member or another individual.
- Abortion – when the minor is considered mature enough to make the decision or if she can show it is in her best interest. A healthcare provider may not tell the parents without the minor's consent.
- Birth control and pregnancy testing – if failure to provide such services would create a serious health hazard or if referred for such services by a physician, clergyman or a planned-parenthood agency.
- Emergency contraception – parental consent is not required.
- Emergency care.

When a minor consents to treatment on his or her own behalf, it is important to understand the required confidentiality of the related PHI and to whom health information may be released. If the patient does not consent to releasing information to the parents, remember to obtain alternate contact information, inform the billing department of alternate contact information, and, if possible, inform the insurance company to treat the billing information as confidential. HIPAA follows state law in that if a minor is able to consent to his or her own medical treatment, then PHI may be used and disclosed without parental consent, but with consent of the minor where consent is required.

As a best practice, consider including on your patient consent forms whether a minor is providing consent for his or her own treatment and, if so, what alternate communication means should be used.

7. External Rotators - Mobile Devices

Okay, so we are not using rotary phones anymore, but we are still communicating with patients when they are not in the office. Complying with HIPAA does not mean that you cannot use your mobile phone or device to discuss patient care. Rather, you need to understand how to protect PHI and e-PHI in doing so.

The Department of Health and Human Services offers these tips for practitioners:

- Install and enable encryption to protect PHI stored or sent by mobile devices.
- Use a password or other user authentication.
- Install and activate wiping and/or remote disabling to erase data on the mobile device if it is lost or stolen.
- Disable and do not install or use file-sharing applications.
- Install and enable a firewall to block unauthorized access.
- Install and enable security software to protect against malicious applications, viruses, spyware and malware-based attacks.
- Keep your security software up to date.
- Research mobile applications (apps) before downloading.

continued on page 8

continued from page 7

- Maintain physical control of your mobile device. Know where it is at all times to limit the risk of unauthorized use.
- Use adequate security to send or receive PHI over public Wi-Fi networks, which are often unsecured.
- Delete all stored health information on your mobile device before discarding it, turning it in for a new phone, etc.

8. Happy Baby - Baby Pictures

Happy Baby is a feel-good stretch! And what feels better than posting those happy baby pictures on the walls in your office?! Some recent articles have suggested that doing so is a violation of HIPAA and some pediatricians have done away with the wall of fame or have hidden it from public view. But do you really have to hide that wall of happy babies? Arguably, the photos are not PHI if a third party cannot identify the patient from the picture and, arguably, pictures in the waiting room would not be a breach as it seems unlikely that someone would be able to retain the information to be able to identify a particular baby.[2] To erase all doubts, a quick reference in your patient consent form for authorization to post baby pictures, and a corresponding description in your notice of privacy practice, should suffice.

9. Keep it up!

Now that you've got your basic HIPAA workout plan – do not stop!

For more information on HIPAA, including training materials, please visit: **www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities.**

And for "fun" games to test your compliance, check out: **www.healthit.gov/providers-professionals/privacy-security-training-games.** ■

1. Treumann, Julie. "Are you Hip to HIPAA?: A Pediatrician's HIPAA Workout Guide for Compliance, Stability and Balance (Part I)." *CCPA News* Winter/Spring 2015: 4-6. Print.

2. Litten, Elizabeth. "Is that Cute Baby Photo Really PHI? Calming the HIPAA Hullabaloo." hipaahealthlaw.foxrothschild.com. **http://hipaahealthlaw.foxrothschild.com/2014/08/articles/privacy/is-that-cute-baby-photo-really-phi-calming-the-hipaa-hullabaloo** (accessed August 26, 2015).