Inside this Edition.............

Integrating Physician Practice Risk Management          Pg 2
Security Breaches, Are You Ready?                       Pg 4
Roses are Red, Violets are Blue                        Pg 8
Identifying Risks in Strategic Partnerships            Pg 11
Taking Your Restraint Program to the Next Level       Pg 12
Integrating Physician Practice Risk Management into a Hospital Based Risk Management Program

Amy Wasdin, RN, MBA, CPHRM
Patient Safety Risk Manager, Southeast Region
The Doctors Company

Over the past decade the healthcare industry has seen an upward shift in the number of physician practices being acquired by hospitals or healthcare care systems. Even though the industry has experienced this trend in the past, the current cycle is unique due to a few new factors:

1. New physicians entering the work force are more interested in maintaining a work-life balance and do not want to be burdened with the responsibility of managing an office setting.
2. Regulatory changes are pressuring the establishment of Accountable Care Organizations (ACO’s) and a value based payment system.

Incorporating a physician practice risk management program

It can be a daunting challenge for a potentially already overtaxed hospital risk manager to realize that he or she is also going to be responsible for overseeing the risk management program for a number of physician practices that the hospital has just acquired. Incorporating physician practice risk management into an already existing hospital risk management program is challenging even for a seasoned risk manager as most hospital risk managers do not have a background with physician practices or a medical office setting. Therefore, it is important from the beginning to become familiar with the risks associated with a physician practice setting.

The risk manager should first identify the areas of knowledge deficit involving the physician practice setting and work to develop resources that will enhance his or her ability to provide effective risk management services. In order to be successful, a risk manager must have “buy in” from the top leadership of the organization and must clearly understand the scope and expectations of what he or she must accomplish.

Depending on how large the physician practice entity is or is planning to become, it is important to establish priorities. A hospital risk manager is usually conditioned to working with limited resources including, but not limited to, staffing. However, no two risk management departments will look the same due to an organization’s operational plan so it is often difficult to find data to support the number and type of resources needed.
How to assess risk – before and after acquisition of a physician practice

It is important to understand the operation and environment of the practice prior to or immediately after the acquisition so that you can best prepare to mitigate and manage the risk that will be associated. The type of risk assessment one should perform depends on the scope of the risk management program—is it limited to loss identification and prevention or does it include claims management as well? Is it limited to a specific type of risk management, such as clinical, or does your responsibility reflect more of an enterprise risk management approach? A general risk assessment of the practice is recommended. The assessment should include a look at how the following processes function in the office setting:

- **Communications** (with patients and among staff): Access, timeliness, protocols.
- **Lab tests, procedures, referrals to specialists, and reporting of diagnostic results**: Use of protocols, documentation.
- **Patient scheduling and follow-up**: System for reminders, protocol for noncompliance, documentation.
- **Medical records**: Type, continuity of patient care evidenced.
- **Medication management**: Documentation, patient education, storage, labeling.
- **Physician/Patient/Staff relationships**: Direct interactions, training and supervision, patient satisfaction.
- **Informed Consent and Refusal**: Review of forms, documentation of patient-provider conversations regarding procedure.
- **Clinical procedures**: Patient identification and verification, diagnostics, sedation/anesthesia, pain management, operative procedures.
- **Confidentiality and privacy**: Measures taken to ensure patient privacy, storage of patient medical records, Notice of Privacy Practices, communication of patient information.
- **Emergency procedures**: Medical emergencies, drills, aggressive behavior.
- **Credentialing and staffing**: New hire orientation, written policies and enforcement, signed acknowledgements, performance reviews, scope of practice.
- **The work environment**: Safety, infection control, security, equipment.
- **Systems and Processes to reduce the impact of human factors**: Addressing fatigue, overwork, stress, and over-reliance on memory.
- **Business Operations**: Patient complaints, billing terms and conditions, audits, corporate compliance, email, computers and mobile devices, social media.
- **Miscellaneous Risk and Loss Control issues**: Patient termination, claims management, event reporting, contract management, advertising, monitoring and evaluating operations.

(See “Interactive Guide for Office Practices” at [www.thedoctors.com](http://www.thedoctors.com)).

**Determine what resources are needed**

The amount of resources required will be determined by the scope of the physician practice risk management program. If hiring additional risk management staff is not an option, it is imperative that the physician practice managers assume ownership of the day to day risk management responsibilities of the practice. This will require the hospital risk manager to educate the practice managers on the principles of risk management and expectations involved such as reviewing incident reports, performing follow-up on reported events, trending data, and communicating risk management information and education to their staff. Larger healthcare organizations may have the financial resources to provide a risk manager to have a more “hands on” approach to managing and addressing the risk management needs of multiple physician practices.

**Consider these tips:**

Develop an understanding of the scope of your responsibilities for physician practice risk management.

1. Utilize educational resources to learn about the operation, risks and regulatory requirements that are unique to the physician practice setting as opposed to the hospital setting.
2. Establish priorities for a physician practice risk management program.
3. Determine what resources (if any) will be available to you in the physician office setting.
4. Establish a risk management plan for the physician practice environment.
5. Seek buy-in from your leadership and the physician practice management leaders on your plan and the resources you will need.
6. Communicate your plan to the stakeholders of the risk management program (i.e., who will be involved and/or impacted by this program?).
7. Provide education on important risk management and patient safety topics, as well as risk management processes such as event reporting.
8. Provide feedback according to your program plan. This may include the Board, a quality improvement committee, practice managers, physicians, and staff members who report events.
9. Involve your professional liability insurance carrier in knowing your needs and concerns. Often there are helpful risk management resources that can be provided to you at no additional cost.

Utilizing these risk management techniques will assist you in establishing the framework for a successful physician practice risk management program within a hospital based system.

*******************************************************************************

SECURITY BREACHES – ARE YOU READY?

Sue Wedemeyer RN, BSN, MBA
Sr. Risk Management Consultant, Risk Engineering
Zurich North America

As healthcare organizations cast their nets out farther and farther to provide service and remain competitive; as mergers, acquisitions and affiliations remain a part of the healthcare landscape; as technology advances and use of mobile devices continues to rise and as dishonest behavior becomes more sophisticated, data breaches are predicted to continue at an increasing rate.

According to the most recent information from Ponemon, the cost of a data breach per capita in the US is $188 with a total cost per data breach of $5.4 million. Healthcare ranked #1 in per capita cost for a data breach out of 15 industries studied.¹ System errors and human factors represent the primary causes of security breaches with the most costly breaches resulting from malicious and criminal attacks. The cost per record from these attacks was deemed to be $277.²

It is globally recognized that cyber-attacks are becoming a more common occurrence. One study of 60 companies reported an average combined total of 122 successful attacks per week in 2013, an 18% percent increase from 2012.²

Accounts of security breaches are reported regularly and often.

Patient records from a California hospital system containing names, birthdates and social security numbers of 4,500 patients were discovered by police during a drug bust. A spokesperson would not comment on whether the information was found in electronic or paper form. The organization’s computers were encrypted six months prior to the discovery following an incident of stolen laptops.

A portion of Microfiche meant for shredding by the vendor was found in a park and contained names, addresses, medical record numbers, clinical information, and some Social Security numbers.

At the end of 2013, a dermatology practice agreed to pay $150,000 to settle violations of the 1996 HIPAA Privacy, Security, and Breach Notification Rules with the Department of Health and Human Services. They will also be required to implement a corrective action plan to correct
deficiencies in its HIPAA compliance program, including a risk analysis and risk management plan and an implementation report to OCR. The breach occurred when an unencrypted thumb drive was stolen from a staff member’s car. “This case marks the first settlement with a covered entity for not having policies and procedures in place to address the breach notification provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of American Recovery and Reinvestment Act of 2009 (ARRA).” The HHS press release can be accessed at: http://www.hhs.gov/news/press/2013pres/12/20131226a.html

Identification of all potential sources of data leaks, no matter how small or unlikely the source may seem, is at the center of any data security program. Frequently cited causes of data breaches are stolen laptops, information inappropriately accessed by an employee, misplaced files or electronic storage and scams or on-line hacking.

INFORMATION ON THE MOVE
It is no surprise that the increased use of mobile devices translates into an increasing security risk. BYOD (Bring Your Own Device) is prevalent throughout healthcare organizations. CTIA, the wireless association, has reported that 2.19 trillion text messages are sent annually. Provisioning and access policy management, virus and malware protection, and prevention and encryption and other data loss technologies are often cited as major concerns when managing mobile devices. It is noteworthy that 29% of respondents to a recent study said they do not take steps to secure employee-owned mobile devices.

The following guidelines have been put into place by the VA to manage mobile devices.

- When a VA device is lost, a user has one hour to report the missing device to the information security team. The data can be wiped off the device by the team and reinstated if the device is recovered.
- Every device must be encrypted.
- Use the software feature that prevents a screen from being copied, photographed or forwarded.
- Make sure a complex password is used that includes letters, numbers and symbols. Make sure it’s changed every three months.
- Adequate training is essential. The VA requires every employee to go through refresher training every year, and if they run over the one-year deadline to schedule training, they are locked out of the system.

THE AFTERMATH
The aftermath of a data breach can be devastating. The reputation and image of an organization may be “on the line” depending on the facts surrounding the breach. In any case, the event often provides story material for the media and much unwanted publicity. The financial impact will vary but can be substantial. Even if the result of the breach does not cause much damage, reporting, notifications and related activities can be costly. In addition, the potential for medical identity theft resulting from a breach is very real. The bottom line, there needs to be a plan for damage control.

MEDICAL IDENTITY THEFT
A recent Ponemon study on medical identity theft states that this activity is on the rise and validates that it is a costly and time-consuming to resolve. Their preliminary numbers for 2013 indicate there have been 1,836,312 victims of medical identity theft, an increase of more than 330,000 from their previous study. The study estimated...
that total out of pocket cost to victims who had to pay was approximately $12.3 billion. Thirty-nine percent of those healthcare organizations that experienced medical identity theft in their organizations say it resulted in inaccuracies in the patient’s medical record and 26% say it affected the patient’s medical treatment.\(^6\)

Clearly written policies and procedures and training of appropriate personnel are basic but important strategies to mitigate potential losses from medical ID theft. Additionally, development of a medical identity theft program and a medical identity theft team to respond to a potential or actual incident is worth consideration.

**BREACH FATIGUE**

With breach notices anticipated to increase in large numbers, it is speculated that “breach fatigue“ will affect a larger number of the population. Consumers’ attention may wane given the constant surge of breach notifications and as a result may not take necessary actions to protect themselves from identity theft. In 2012 alone, one quarter of the U.S. population received at least one letter notifying them they had been breached. “The worst case scenario in the healthcare sector could find someone failing to take action when their healthcare identity has been stolen. Then, when they go in for a procedure or treatment, their medical records could contain incorrect information. All sorts of medical errors and complications could be the result.”\(^7\)

Breach notifications need to be clear and distinct in the message they convey and notifications need to encourage action on the part of the consumer. There may be times when further means are necessary to deliver the message to the public. A sample breach letter can be found at:


**REGULATORY ENVIRONMENT**

In 2013 The Omnibus Rule introduced some sweeping changes. In addition to strengthening a patient’s privacy rights and protections, the “Rule” affords increased ability to enforce the HIPAA privacy and security protections.

A partial list of the changes includes, broadening the definition of a data breach; requirements to update public patient-privacy rights reporting and train staff on the changes; a requirement that healthcare providers revise their notice of privacy practices and expansion of liability for business associates covered under HIPAA.

With regard to business associates, organizations should vet all vendors to ensure HIPAA compliance, review the vendor’s history with PHI security, confirm vendor knowledge of the severity of penalties for a breach and evaluate communication channels so that patient data is protected as it is transferred between entities.

**MANAGING THE RISK**

For hospitals and health systems, safeguarding communication of electronic protected health information, or ePHI, should be part of an overall organizational risk management strategy. Ideally, the momentum behind this would be a security committee with representatives from the entire organization including information technology and health information management, senior administration, risk management, operations, medical staff and nursing, as well as legal counsel. It also may be appropriate to hire an external security firm, depending on the security expertise of the committee members.

There is no “one size fits all” method for addressing a security breach, although “be prepared” is a common thread. However, numerous strategies have been identified to guide the identification and management of these events.

- Appoint an information security officer at the senior administrative level
- Regular meetings between information security and senior administration
- Promote environment of open communication
- Risk assessment of data sources and transmission points, including historic data contained in paper files, floppy disks, etc. Determine where data “lives” within the organization.
- Education of leadership and staff
- Implementation of encryption technology
- Incident response plan including business associates
- Benchmarking of security practices
- Well drafted organizational policies and procedures, including BYOD policies
- Development of Cloud security policies
- Mock breaches, including table-top drills
- Restrict employee access to data

**FACING THE FUTURE**

The sources of potential data breaches are increasing rapidly with the growth and expansion of healthcare organizations and the increasing use of technology and technological devices. The healthcare industry provides a substantial target for security breaches and it stands to get larger once the Healthcare Exchanges are fully operational and infuse millions of people into the healthcare system. According to Ponemon, “the healthcare industry will be the most susceptible to data breaches, which will most likely be publicly disclosed and closely scrutinized.” Be prepared is not just an idle warning. It is a must do.

2. Data Breaches\Study Cybercrime Costs Grow 26\% HealthcareInfoSecurity.mht

The information in this publication was compiled from sources believed to be reliable for informational purposes only. All sample policies and procedures herein should serve as a guideline, which you can use to create your own policies and procedures. We trust that you will customize these samples to reflect your own operations and believe that these samples may serve as a helpful platform for this endeavor. Any and all information contained herein is not intended to constitute legal advice and accordingly, you should consult with your own attorneys when developing programs and policies. We do not guarantee the accuracy of this information or any results and further assume no liability in connection with this publication and sample policies and procedures, including any information, methods or safety suggestions contained herein. Moreover, Zurich reminds you that this cannot be assumed to contain every acceptable safety and compliance procedure or that additional procedures might not be appropriate under the circumstances. The subject matter of this publication is not tied to any specific insurance product nor will adopting these policies and procedures ensure coverage under any insurance policy.

© 2014 Zurich American Insurance Company

**************************

Visit www.gshrm.org to register for the June 4-6 annual conference!
Roses are Red, Violets are Blue, if the Love Language Works at Home, then Why Not at Work, too?

By James Ruffin, Ph.D.
James Ruffin Consulting

Can hardly believe it's February...again. Just as all the hustle and bustle of the holidays die down, the day of love looms around the corner. Not only Valentine's Day, as if that's not enough, but in my case, the celebration of our wedding anniversary, too. Yes, two whammies back to back in the same month. So, not only does Cupid here need to come up with some grand gesture of love and affection, I must also show in the most thoughtful and memorable way as possible, my continual love and devotion as I remember the day of our wedded bliss. (As if I could forget.) In our home, a wall calendar hangs in the kitchen marked with those not-so-subtle February reminders, including bold red hearts marked around the "don't forget or else dates".

So, as I ponder gift ideas, I begin to think about what's really important in a good relationship. Things like, our time (in my case, it's sitting through a romantic movie), careful attention, (remembering her favorite flowers or buying something she may have spotted in a store) and most importantly, being a good listener (a quiet dinner for two). Essentially, being a good communicator is offering the gift of yourself and is required in order to cultivate and maintain any good relationship, whether in love, friendship, or work. So in honor of Valentine's Day, let's take some of these relationship adages and see how these same truths that apply in love, can also apply in a work setting, and in particular, for the healthcare risk manager.

Finding Mr. (or Mrs.) Right.

As a risk manager, your job description is filled with tasks, but possibly the most important is that of the go-between. When you are called into action by the hospital, it is most often because a claim by the offended party has been filed. Through no personal fault of your own, you are required to step in and act as mediator for the two opposing groups, usually a patient and/or family member and doctor and/or hospital. In what is typically a high stakes negotiation, possibly involving millions of dollars, the most effective person should be sent. One who can broker an agreement between the parties to lessen the damages or settle without the additional cost of further litigation or trial. In a sense, the risk manager is the first and last chance for a peaceful and mutually agreeable resolution.

Taking a practical approach for a moment. I know that if my wife and I had a disagreement and I'd like to make things right, I certainly would not have my secretary deliver roses and a message to her. No, I'd go myself! Neither would sending just anyone to a high stakes negotiation. Sending the right person for the job is paramount. Does the case involve a slow speaking, elderly farmer from Mississippi? Let fast-talking, big city "Joe" from New York sit this one out. Or,

---

From Dr. Seuss

Unless someone like you cares a whole awful lot, nothing is going to get better. It's not.

*****

Think and Wonder. Wonder and Think.

*****

Sometimes the QUESTIONS are COMPLICATED and the ANSWERS are SIMPLE.

*****

You don't have to brush all your teeth, just the ones you want to keep.

*****

Don't cry because its over. Smile because it happened.

*****

Why fit in when you were born to stand out

*****

You're off to Great Places! Today is your day! Your mountain is waiting. So...get on your way!
does the case involve a child? Consider sending someone who is a parent themselves, one who can start to build rapport simply based on commonality alone.

Finding Mr. or Mrs. Right for the job is the first step to successful negotiations. Sending the wrong person could eventually cost dearly.

**It's not what you say, it's how you say it.**

Okay, so consider yourself the lucky one, the Mr. (or Mrs.) Right risk manager sent in for the job. Do you act like you're dragging the ole ball and chain, or do your words and actions marry (no pun intended)? After many years together, I know that when I ask my wife how her day was, even if the same answer is, "Fine", I can tell by tone, action, and inflection what she really means by that. As a matter of fact, most anyone, even if they never spent more than a few minutes with my wife, would know what kind of mood she's in and whether or not she really had a "fine" day. That's because most of our communication is based on non-verbal responses rather than the actual words that are spoken. In fact, 55% of our message is delivered by body language alone, followed by 38% in voice tone and inflection, and of the actual words, only 7%!

For risk managers, or anyone else for that matter, to be effective communicators, body language, including facial expressions, and voice must mirror what is being said. For example, when speaking with a patient or family member, you may offer some sort or verbal condolence but, do you merely say it, or mean it? If you look into their eyes, maybe reach out physically to them in some way, or just stop what you're doing to listen, then you will have initially established rapport and a good foundation to build upon when emotions start to run high. If you are distracted, maybe answer your phone at an inopportune time, seem fidgety, vocally rushed or even fail to make appropriate eye contact, then rest assured, you will be taken as disingenuous. Even if your words express empathy, remember it's not what you say, it's how you say it.

Other times, it's not what you say at all.

**Silence speaks volumes**

I'm not talking about the kind of "silent treatment" you may get at home. You know, the punitive, not speaking just to annoy you type silence. Or even the silence of being a good listener, although also very important. No, here I'm talking more of the movie-type quiet, where "Silence is Golden". Most people would rather fill a silent conversational gap with meaningless small talk and chatter, just to avoid that awkward silence. But in the case of negotiations, silence may be your best approach when enough has already been said. As a matter of fact, limiting what you say can significantly work in your favor, particularly in a situation where a risk manager must investigate a claim. During the interview process, you give information when you speak. Thus, the patient/family member or representative is in control because they are receiving information. Conversely, when you allow the interviewee to speak, they are in the "hot seat" of delivering information, both verbally and non-verbally, and the risk manager/ interviewer gains control. In addition, knowing when to be silent is just as important as knowing when to speak. During highly emotional times, cognitive skills, analytical thought and memory are diminished. More specifically, Elisabeth Kübler-Ross identifies grief in stages. They are denial, anger, bargaining, depression, and acceptance. The conversations or questioning of a patient/family member during a time of loss or sadness will inevitably fall into one of these stages. If a risk manager has taken the time to build rapport during initial conversations, then they will be able to correctly identify what stage of grief a person is in and adapt what they say or do accordingly. Therefore, knowing when to ask questions or conduct an interview is just as important as knowing when not to say anything at all.

**Say what you mean and mean what you say.**

As risk managers, building truth and rapport may be the most important step in developing and maintaining a good relationship. Without it, you will inevitably fight an uphill battle. That's because if someone doesn't trust you, they will not communicate with you openly and if they don't communicate with you openly, then you will have lost your opportunity to negotiate effectively.
Stop and smell the roses………

It seems like a new year brings new resolutions that folks may or may not follow complete. Stress seems to affect everyone and is very normal but when your body stays in a constant state of stress, it can lead to serious health issues. Although we all know about stress, we don’t stop to take the time to evaluate what may be causing it or what we can do to reduce it. We all have busy jobs with a lot of responsibility and are trying to do more with less staff. That is the nature of healthcare and is not going to get better.

Everyone handles stress differently. For some, stress is what they need to get a deadline completed. For others, it totally shuts them down and they can’t even meet their deadline, causing more stress.

There are many ways to help reduce your stress level. Finding out the source causing the stress is the first step. Once you identify the cause, look for ways to manage it.

Managing stress may mean managing your time differently, talking to a friend or professional, getting more sleep and learning to say no!!

Ways to relieving stress can mean exercising, listening to music, laughing or taking more time away from work. Get creative and do what works for you!!

While at the annual meeting, treat yourself to a visit to the spa, ride horses, walk the many trails or hang out at the pool with your friends (when the meetings are not in progress of course!!)

Stop and take some time for yourself. You are worth it!!

So, how do you build trust in a relatively short amount of time? The same way you would act after a first date. That is, if you wanted a second. Beyond making a good first impression, say what you mean and mean what you say. Though it may seem trite, opinions about us are formed very early on in a relationship and the little things matter. For example, a risk manager may tell a patient they will "call them back", but never does. Now, most people would not hold the risk manager accountable for this oversight as we have all sometimes fallen short in following through. But for that risk manager to actually do something he or she said they would do and in a timely manner will work wonders in building trust. The patient will see you as a person who cares about the little things and in turn, will begin to trust you with the bigger issues. Your credibility soars and over time of being consistently reliable, they will view you as a person of integrity who has a sincere interest in others.

Are you ready to say those three little words?
Hint: It's not "I love you." Sweet nothings aside for a moment, the most valuable words one can say to another during the delivery of a negative message is simply, "I am sorry." This does not necessarily mean an admission of guilt to some wrongdoing, so lawyers simmer down a moment. What I mean is the act of being genuinely regretful over something that has happened, or an apology for the situation. "I am sorry that you are having to go through this. I will do my best to help." Or, "I am sorry for your loss." Not seeking forgiveness, but showing genuine sympathy.

You had me at, "Hello."

If you know that famous line came from the movie, Jerry Maguire, then like me, you may have seen far too many chick flicks, more than you care to admit. But, it brings me to my conclusion for the risk manager. If the love language works at home, then why not in the workplace, too? Not the romantic, I'll meet you at the top of the Empire State Building on Valentine's Day love, (tissue, please) but the agape, brotherly love of genuine care and concern. First impressions, thoughtful words, and timely actions make the all the difference. Go ahead, Romeo, give it a try! Happy Valentine's Day!

************************************
Identifying Risks in Strategic Partnerships

By Maryann McGivney
Executive Vice President, Willis Insurance Services

The Affordable Care Act (ACA) was passed by Congress and signed into law on March 23, 2010. Despite many challenges, debates, and general confusion, the law set into motion changes in the US Healthcare Delivery system of unmatched proportions. Almost 4 years later, we are beginning to see the impact on our delivery model. One of the most significant results impacting the ‘business of healthcare’, is the formation of new and creative strategic partnerships between healthcare providers. These partnerships follow no traditional or common thread and are as unique and creative as the partners designing them. Some of the more common arrangements include ACOs, Health Information Exchanges, partnerships between Health Systems and Health Plans, Joint Ventures, Management Agreements, Clinically Integrated Networks, Technology Sharing/Leasing, and even support for local employers with self-insured medical plans.

For Risk Managers, who are often not part of the initial dialogue, these partnerships are creating new and unusual risks that need to be managed, and often after the decision is made. Identifying and assessing these exposures can be a daunting task, but an even more challenging endeavor may be determining how commercial insurance may or may not cover the risks. As you evaluate the arrangements between your organization and others, consider the following points.

**Identify the Structure** of the Partnership or Affiliation. What services are being provided by each party? How are the organizations connected? Is there any ownership interest or are the relationships all third party? Written agreements can help to alleviate confusion later. While written agreements take some time and negotiation, they play a key role in evaluating the responsibility of each party. Often the written agreement contains all of the information that underwriters will require in determining coverage or crafting endorsements. It is not unusual for an underwriter to require a copy of the written agreement(s) before agreeing to endorse or change coverage. As you work with your insurance carriers, pay particular attention to the coverage triggers. For instance, most Healthcare Professional Liability (HPL) policies are triggered by a ‘Bodily Injury’. If the contract makes you responsible for the other parties’ “Financial Loss”, and you endorse the activity onto your HPL policy, you may not have the coverage that you really need.

**Determine Financial Responsibility** – As you consider which parties will be responsible for which liabilities, be sure to consider what you would be ‘on the hook’ for anyway. Many organizations try to push financial responsibility to other parties in a written agreement. However, you may not be able to legally accept, or pass on certain responsibilities. For example, if you own patient data for a certain population, you may not be able to fully transfer the risk of data breach to another entity. In addition, particularly for larger organizations, as much as you would like to have another party assume the financial responsibility, your asset size and/or control of the arrangement, may make you the target regardless of the contract wording. Legal input should be sought for all arrangements to be sure that your organization is adequately protected and understands the implications of the agreement.

**Evaluate Contractual Wording and Insurance Requirements** – There are situations where a vendor or partner is not flexible in the written agreement. They may refuse to negotiate wording, or insist on certain coverages and coverage limits. While this is not the ideal arrangement, underwriters do understand that sometimes business decisions are made based on the long term benefits which may outweigh the debated language. It is particularly important in these situations to seek the feedback of your underwriter and/or broker to determine if you can live with the requirements being demanded. Pay particular attention to contract wording that requests specific coverage terms or could be limiting to the coverage that is available. For example, many underwriters will often include wording in their policies that caps the carrier’s responsibility in a contractual arrangement at the limits required in the contract. Therefore if your contract requires $1M of HPL coverage and there is a large loss, your insurance carrier may argue that they are not responsible for anything over $1M. An easy remedy is to re-word the contract such that the limits required are not capped at any particular amount.
Assess Your Current Coverage – Historically, contracts and agreements were as simple as checking off a list of coverage types and limits, with the occasional need to consider retro dates or tail coverage. With the uniqueness of today’s arrangements, the checklist is only the beginning. First, if your organization does utilize a checklist or template for agreements, now is a good time to review the insurance requirements. Have you added provisions for newer coverages such as Network Privacy, Regulatory Liability, Management Errors and Omissions and Technology Errors and Omissions? Are the limits still adequate for the exposures? Are there any specific coverage terms that should be required (for example Primary and Non Contributory, or whether or not the Insured versus Insured provision needs to be amended)?

Second, where your organization is responsible for the arrangement, consider how these new exposures will impact your own insurance and risk program. Should you consider different retentions or limits? Would it be better to purchase ‘stand alone’ coverage to protect your loss run or as part of your exit strategy should the partnership fail?

Coordination of Services and Best Practices – Ultimately any partnership needs to function in a cohesive fashion in order to be successful. Sharing may be a new and uncomfortable activity for one or all parties. Consider how information sharing and Best Practices can be implemented, particularly when it comes to identifying incidents and potential claims. Who is ultimately responsible for notifying the group regarding claims activity? Who makes the decision as to the reporting of claims to commercial carriers? Once a claim is reported, who makes the decisions on how to handle the claim, and how will others be kept informed of the process? If purchasing a ‘stand alone’ product, who makes the decision on what coverages and limits to purchase?

The New World of Strategic Partnerships in Healthcare will lead us to a new and improved way of caring for the US population. In the meantime, the Risk Management role is becoming considerably more challenging. There is a tremendous opportunity when your organization embarks on a Strategic Partnership to demonstrate the Risk Manager’s (or Risk Department’s) knowledge and contributions to the organization. The success of these partnerships not only depends on your input, but can help to elevate your visibility and support within the organization.

********

Taking Your Restraint Program to the Next Level: Strategies to Address Common Causes of Preventable Patient Harm and Death Associated with Restraint Use

Caroline Brill, RN, BSN, JD, CPHRM, FASHRM
AVP, Healthcare Risk Management-AWAC Services
Allied World Assurance Company, LTD

There may be times when a patient will require the use of restraints in order to prevent injury to himself/herself or others, or to prevent interference with his/her treatment. Generally, restraints include physical/mechanical devices used to reduce or restrict a patient’s mobility. Other types of restraints may also include medications used to
control the patient’s behavior, and items designed to keep a patient in bed or prevent him/her from getting up. The Centers for Medicare and Medicaid Services (CMS), The Joint Commission and many states have developed regulations and standards for use of restraints and each carefully monitors adverse events that occur with restrained patients.¹

A 2012 German study analyzed autopsy reports from the Institute of Forensic Medicine in Munich from 1997 to 2010. The results revealed 26 cases of death while the individual was physically restrained.²

The root causes included:

- Lack of continuous observation by clinical staff
- Restraints incorrectly fastened
- Use of non-standard restraints iii

Similarly, here in the United States, within just over a six week period, six patients died in a Pennsylvania hospital following the use of chemical or physical restraints.³ These figures are alarming and it can be surmised that a number of these deaths could have been prevented.

The implications associated with the use of restraints are apparent. However, it is often difficult for care providers to balance the need to use restraints in order to protect the patient or others from serious harm and keeping those very same measures from causing significant injury or death to the patient. In addition, clinicians must simultaneously consider and maintain practices that uphold patient’s rights principles.

Risk mitigation strategies designed for the use of restraints in the health care setting begin with following the regulations and/or guidelines provided by legal, regulatory, and accreditation agencies. As previously mentioned, CMS, accreditation bodies, state laws and industry standards provide mandates and guidelines for the appropriate use of restraints designed to protect patient safety and patient rights.

However, merely adhering to guidelines and mandates has not proven effective enough to prevent serious injury and death associated with restraints. Despite the many regulations adopted, improper use of restraints and inadequate patient observation and monitoring have emerged as key areas to heed and address in order to elevate your restraint program to the next level.

**IMPROPER USE OF RESTRAINTS**

According to the federal rules, a patient may not be restrained for “coercion, discipline, convenience, or retaliation by staff.”⁴ At times, clinicians may be tempted to use chemical or physical restraints for their own convenience without consideration for other means to control a patient’s behavior. Or, at other times, staff may restrain a patient to force him/her to take a medication or complete a procedure. In these latter situations, there can be a very fine line between the proper use of restraints and a violation of a patient’s rights.

“Taking down” an aggressive patient is another situation presenting a “dangerous territory” from both the patient’s rights and patient safety perspectives. From the patient safety aspect, many strategies used to effectively hold a patient down may restrict oxygen to the patient resulting in suffocation. To reduce patient harm in these situations, only designated staff members who are properly trained in nonviolent crisis intervention should be permitted to “take down” and physically restrain a patient after all reasonable alternative means (e.g., de-escalation techniques) have been exhausted or less restrictive means have been determined to be ineffective. Additionally, the use of restraints should be individualized, taking into account a patient’s specific physical/psychological difficulties. From the patient’s rights perspective, staff should be able to readily determine that the rationale for using such measures was to protect the patient or others from imminent and significant harm and not to punish a patient for displaying certain behavior.

Restraints and/or seclusion may be appropriate when “… according to clinical judgment, less restrictive interventions are inadequate or inappropriate and the risks of these interventions outweigh the benefits.”⁵ The risk/benefit analysis involves focusing on the behavior at issue, considering all possible measures available, and
analyzing each potential measure to determine which may be the least restrictive yet most effective to attain the goal. Documentation should properly reflect the clinician’s risk/benefit analysis that supports that the proper restraint has been utilized and least restrictive measures were considered.

Sometimes the need to use restraints must be made in a split second in the interest of keeping the patient or others from immediate and significant harm, particularly in the emergency department or behavioral health unit. When faced with these split second decisions, an objective agitation assessment scale, such as the Overt Aggression Scale, may be utilized as a factor to determine whether restraints or seclusion may be immediately necessary.

Regardless of the clinical area where restraints may be utilized, formal processes that guide the risk/benefit analysis will facilitate proper restraint usage. According to the American Nurses Association (ANA), citing The Joint Commission, “Seclusion and/or restraint may be more likely to be employed inappropriately – that is, for non-emergency situations or circumstances where no significant risk of harm exists when hospital unit staffing is inadequate or the staff is inappropriately trained to provide less restrictive interventions.”

An individualized approach should include a systematic assessment that includes an evaluation of the underlying causes of the patient’s behavior. At that point, caregivers should incorporate the treatment designed to address the identified underlying causes of certain behavior, into the patient’s plan of care. The ultimate goal is to eliminate the need for restraints.

Another way to reduce the use of restraints is to enhance annual staff education and training by facilitating brainstorming sessions to identify options for less restrictive interventions for different scenarios when a patient may require restraints. Begin by discussing various behaviors (e.g., pulling, scratching, frequent falls, agitation/aggression, wandering) and identify several alternatives to restraints for each given behavior.

**INADEQUATE PATIENT OBSERVATION AND MONITORING**
The Agency for Healthcare Research and Quality reported that hospitals with low nurse staffing levels tend to have higher rates of poor patient outcomes, including: pneumonia, shock, cardiac arrest, and urinary tract infections. The report isn’t shocking because common sense tells us that inappropriate nurse-patient ratios leads to poor care, including when restraints are used. Listed below are just a few examples of restraint deaths associated with inadequate staffing levels and lack of patient monitoring:

The root causes of a chemical restraint death in a Missouri hospital included failure to monitor the patient and inappropriate staffing levels.

At a Pennsylvania hospital, a patient was found partially dangling from her bed while wearing a vest restraint. The patient’s family successfully sued the hospital for wrongful death after the patient died from asphyxiation from a vest restraint. A review of the medical record revealed several late entries. The multiple late entries may have suggested that the patient was not adequately monitored by staff.

In Georgia, a patient’s body was found on the street below his hospital room window. The patient had been restrained by various methods during his hospitalization and was ordered to have a sitter at the time of the incident. A sitter was not available at the time of the incident.

Facilities can avoid becoming the subject of similar headlines by ensuring that patient care units are adequately staffed and patients who are in restraints are properly monitored at appropriate intervals. To assist in improving patient safety when using restraints, facilities should enhance staffing models by ensuring that adequate patient acuity levels are assigned to patients who are in restraints and evaluate whether the proper use of unlicensed assistive personnel is maximized for each relevant clinical area.

**Risk Management Tips**: 

---

![GS&HRM Logo](http://example.com/logos/gs-hrm.png)
• Ensure that policies and procedures governing use of all restraints/seclusion comply with federal and state laws.
• Educate staff annually regarding assessment, de-escalation techniques, using least restrictive alternatives, and proper restraint application.
• Avoid restraining patients in the prone position in order to avoid asphyxiation.
• Thoroughly document all measures taken including, assessments conducted, least restrictive alternatives used, decision making process leading to restraint use and observations made during restraint use.

Conclusion:
Patients will at times require the use of restraints in order to prevent injury to themselves or to others, or to prevent interference with their treatment. A robust restraint program that addresses all aspects of restraint use, above and beyond minimum regulatory requirements, will promote safe and appropriate restraint usage practices while simultaneously preserving the patient’s rights.

This information is provided as a risk management resource and should not be construed as legal, technical or clinical advice. This information may refer to specific local regulatory or legal issues that may not be relevant to you. Consult your professional advisors or legal counsel for guidance on issues specific to you. This material may not be reproduced or distributed without the express, written permission of Allied World Assurance Company Holdings, AG (“Allied World”).

---

3 Ibid.
5 42 CFR §482.13(e), http://www.ecfr.gov/cgi-bin/text.idx?SID=21bb87d60c5cfe525d3541e965fbb37&node=42:5.0.1.1.2.4.3&rgn=div8, 12/31/13.
12 “Risk Management Pearls, Behavioral Health Across the Continuum,” (2012)