

THE Physicians Report

SUMMER 2013 PHYINS.COM

7
Hospice of North Idaho
talks about its breach

10
HIPAA Q&A:
What you need to know

12
Using social media
under the rule of HIPAA



Making your practice

HIPAA
healthy

Embracing Change

“The only thing that is constant is change,” said Greek philosopher Heraclitus. And here we are, nearly 2,500 years later, and those words ring true today. Medicine is changing at breakneck speeds with advancements in our understanding of the human body. Health care is experiencing tectonic shifts as practice models, patient panels, and payor rules change. And not since the Medicaid and Medicare programs were created in 1965 has our country undergone the type of change proposed by the Affordable Care Act.

Physicians Insurance is changing, too. Not only are we continually working to increase the value and services we bring to members, but we’re also looking to improve communications and enhance how information is shared. This new edition of the *Physicians Report* is just the spearhead of that effort.

Based on focus group research and member surveys, we’ve updated

the *Physicians Report* to help you address changes in the business and practice of medicine. In each edition you’ll find focused, in-depth articles on timely topics, case reviews, and helpful information you can put to use in your own practice. In the months between editions, we’ll send you e-mails of relevant articles and information, keeping you connected to risk management topics and specialty-specific news.

Change isn’t necessarily a bad thing. Without it we would not have the exchange of ideas to together ensure the *Physicians Report*—and Physicians Insurance—grows and adapts to provide the resources that are most relevant for you today.

Though today’s news headlines claim that health care is in a crisis or that the future delivery of care is impossible with today’s models, you can count on Physicians Insurance—the only locally based, mutual company in the Northwest—to be alongside you every step of the way.



Mary-Lou C. Misrahy

Mary-Lou Misrahy, ARM
President and CEO

EDITORIAL STAFF

PUBLISHER
Mary-Lou Misrahy

SENIOR EDITOR
David Kinard

MANAGING EDITOR
Kirstin Williams

EDITOR
Elaine Riordan

CONTRIBUTING EDITORS
Cathy Reunanen, Dr. Robert Oikawa

CONTRIBUTING EDITOR—LEGAL
Gary Morse

STAFF WRITER
Nina Rogozen

ART DIRECTOR
Ron Hansen, Hansen Belyea

ART DIRECTOR
Lynn Anselmi, LA Design

WEB EDITOR
Elaine Riordan

ADMINISTRATIVE SUPPORT
Laura Brosten, Bonny McFarland
Nancy Reithaar

EXECUTIVE MANAGEMENT GROUP

PRESIDENT AND CHIEF EXECUTIVE OFFICER
Mary-Lou Misrahy

**SENIOR VICE PRESIDENT AND
CHIEF INFORMATION OFFICER**
Leslie Mallonee

**SENIOR VICE PRESIDENT,
GENERAL COUNSEL AND SECRETARY**
Gary Morse

SENIOR VICE PRESIDENT, UNDERWRITING
Rick Nauman

**SENIOR VICE PRESIDENT,
CHIEF FINANCIAL OFFICER AND TREASURER**
Rod Pierson

**SENIOR VICE PRESIDENT,
HUMAN RESOURCES AND ADMINISTRATION**
Alison Talbot

BOARD OF DIRECTORS

Brian P. Wicks, MD, Chairman
Ralph A. Rossi, MD, Vice Chairman
Aparna Ananth, MD
Lloyd David
Jennifer Hanscom
John R. Huddleston, MD
Chi-Doo “Skip” Li, JD
David McClellan, MD
Timothy L. Melhorn, MD
John Pasqualetto
Sheila Rege, MD
David A. Russian, MD
Walter Skowronski
Leslie A. Struxness, MD
Josephine Young, MD

READ *PHYSICIANS REPORT* ONLINE
www.phyins.com/Summer2013

CONTACT *PHYSICIANS REPORT*
editor@phyins.com

HOME OFFICE:
Seattle, WA
Copyright 2013

Physicians Insurance A Mutual Company

FEATURES



7 Surviving HIPAA Violations

Learn lessons from Hospice of North Idaho, a local Northwest facility that came out on the wrong side of an OCR audit and emerged stronger and safer.



4 How to Achieve a HIPAA-Healthy Lifestyle for Your Practice

Health security expert Dr. Robert Oikawa charts a disciplined path for approaching HIPAA compliance.



10 HIPAA Q&A: with an Expert

Leslie Meserole, JD, provides insight into compliance documentation and gives advice about making it happen by September 23.



12 Social Media Marketing

Concerns about compliance need not scare you away from social media.

RISK MANAGEMENT

- 14** New HIPAA Self-Study Course: Available Online
- 15** Live Webinar: Social Media
- 15** Washington Laws Effective July 1, 2013
- 16** What's the Fix? Examples of Real-life HIPAA Issues Resolved

MEMBER NEWS

- 18** Board Members: Meet the 2013 Additions
- 19** New Members: Welcome!
- 20** Member Spotlight: Compass Oncology
- 21** Certificates of Insurance: Online and On Demand
- 21** Online User Accounts: Access to a Library of Resources

TRIAL RESULTS

- 22** Arbitration: Voluntary and Mandatory

WE'D LIKE TO HEAR FROM YOU!

Send us feedback and tell us more about what you would like to see in upcoming issues. E-mail us at editor@phyins.com.

How to Achieve a HIPAA-Healthy Lifestyle for Your Practice

BY ROBERT Y. OIKAWA, MD,
MPH, CISSP, CPPS, CPHQ

September usually means back-to-school, football, and glorious dry, sunny weather in the Pacific Northwest. It's the vision that sustains us through the gloom of our long rainy season. But for many practices, this September will be different.

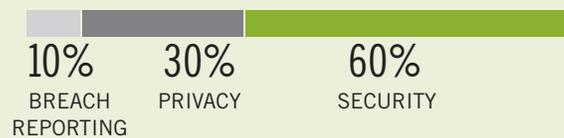
September 23, 2013, is the deadline when all hospitals, clinics, and practices must meet all requirements of the HIPAA Final Rule announced in January. Shortly thereafter, the Department of Health and Human Services (HHS) will begin audits to ensure that everyone meets their HIPAA obligations.

The Office for Civil Rights (OCR) enforces HIPAA. The OCR's 2012 Pilot Audit Program examined 115 organizations, including 61 hospitals and clinical practices of all sizes. Going far beyond a simple checklist, auditors looked closely to see if organizations were truly behaving in accordance with HIPAA by making on-site observations and interviewing clinic staff. *A snapshot of the Pilot Audit Program's results are shown here.*

In April, the OCR presented the Pilot Program findings showing that most health care providers were ill-prepared:

95% of providers had at least one deficiency

Deficiencies involved:



Multiple deficiencies were the rule:

70% had more than 5 findings

40% had over 10 findings

2/3 did not have a complete and accurate risk assessment

Most common cause for a deficiency:

did not know of the requirement

30%



The new tiered penalties for HIPAA mean that, depending on the number and severity of deficiencies found by auditors, or uncovered by OCR during a complaint or breach investigation, your practice could face stiff fines, potentially tens of thousands or even millions of dollars.

Breaches are extremely expensive. Surveys show that data breach costs average \$200 per individual including the costs of notification, credit check services, technical investigation, correcting problems, legal fees, lost opportunities, and reputational harm. The average U.S. primary care provider has about 2,300 patients, so a breach involving all records could easily cost nearly half a million dollars.

Nearly one in four data breach victims suffer identity theft involving credit or financial fraud.* Medical identity theft is more serious because it can result in a patient's loss of coverage and errors in medical records. Other related problems include fraudulent use of stolen provider credentials, theft from practice bank accounts, and even targeting of patients for theft of prescription medications.

We rely on trust-building activities everywhere in our lives. Examples include getting a driver's license, graduating from medical school or nursing school, receiving our professional licenses, gaining hospital privileges, and achieving board certifications. A HIPAA audit measures how well you are meeting your obligations against an objective standard. Passing an audit raises the level of confidence that you, your patients, and HHS have that you are meeting your HIPAA responsibilities. It means that you and your patients can have peace of mind knowing that you have taken all reasonable precautions to prevent breaches. Conversely, failing an audit or having a data breach reduces the confidence others have in you.

HIPAA compliance is a journey, not a destination.

I think of sound security, safety, and privacy practices as the essential "HIPAA-healthy lifestyle." Healthy lifestyles focus on prevention and not remediation. The OCR's audit program shows that most practices are currently out of shape and overweight, with a "HIPAA-unhealthy" lifestyle. Many have never weighed themselves, checked their blood pressure, or asked themselves if they smoke cigarettes. If you're like the majority of practices, you have a lot of work to do between now and September.

Fortunately, clinicians have been advising patients on becoming healthier for a long time. If you think of your practice as the "patient," and the goal as "achieving a HIPAA-healthy lifestyle," you have all you need to get started.

- 1. You must first learn what's required** for a HIPAA-healthy lifestyle, just as a patient must first understand what makes their lifestyle healthy or unhealthy. Remember, the most common root cause discovered by the OCR was "unaware of the requirements."
- 2. Next, assess your unique practice situation** and identify your risk factors. In some cases the problems will be obvious, but in others you may need help from an expert, peer, or outside observer. Some practices may have underlying high-risk diagnoses requiring specific interventions or therapies.
- 3. Decide and commit.** If you opt for a healthy lifestyle and decide to lose weight or quit smoking, you must take personal responsibility to change. Pursuit of HIPAA compliance requires dedication and self-accountability.
- 4. Have a treatment plan and schedule.** Once you understand your situation, you'll need to create a treatment plan to meet the September 23rd deadline.

Like many parts of medicine, there's no single best way to achieve a HIPAA-healthy lifestyle.

- 1. Watchful waiting is contraindicated** because the HITECH Act requires OCR audits. You'll have only 10 days to prepare if you receive a notification letter from the OCR. And, if you have a breach, the damage will have already been done.
- 2. Transfer care** – Sometimes you can transfer responsibility to a specialist, especially with legal or technology matters. However, many activities covered by HIPAA are essential to patient care and are not easily separated. Under the Final Rule, you are ultimately responsible for

the personal health information of your patients, even if you entrust it to others. Make sure that your technology or legal specialists have a HIPAA-healthy lifestyle. One area that you can't transfer is risk analysis.

- 3. Make a referral** – In some situations, you can hire a consultant. Consultants provide advice on how to achieve a HIPAA-healthy lifestyle and may help with special skills (diagnostic testing, facilities, or therapies). Consultants work best when they have a specific diagnosis or problem to address. Aside from cost, the biggest downside is that knowledge, understanding, and skills walk out of your clinic when the contract ends. Beware of consultants selling technology silver bullets that are the HIPAA security version of magic diet pills. To work with consultants, you'll need to be adept at evaluating qualifications (to avoid creating new problems), prognosis (risk analysis), and diagnosing the specific problems they should address.

- 4. Get education** – Self-study and classroom instruction are time-honored methods for continuing education and subject-matter mastery. Books, papers, online training, and class offerings abound. One thing to consider about self-study is the huge abundance and variable quality of content. You'll want to identify who at your clinic should get what training, plus where to start and what to focus upon. Classroom training is an investment of time and money, and you'll want to use the new knowledge promptly to make it stick. Education and self-study materials can sometimes be generic in order to reach a wide audience, so you'll still need to apply your learning to your own situation.

- 5. Use a coach** – Coaching improves motivation, knowledge, skills, abilities, and decision-making with confidence in sports, executive leadership, clinical practice, and professional development. Top executives and world-class athletes often retain coaches to improve performance. Health coaching can change long-term healthy lifestyle behaviors including levels of physical activity, diet, tobacco use, and medication compliance. Coaching excels when setting goals, motivation, sticking to schedules, and developing problem-solving and decision-making skills are needed, and when sustained results are important. Coaching develops expertise within your practice, and is an investment, not a cost. Coaching is less expensive than consultants but more expensive than self-study. The key is to find a coach with the right combination of knowledge, experience, skills, and coaching style. Coaching may be combined with consultants, classroom training, self-study, do-it-yourself, or even outsource arrangements for better, more sustained results.

September is coming quickly. HIPAA audits are on the horizon. You know what you need to do and the options. Commit and get started now!

*Javelin Strategy and Research, 2013 Data Breach Fraud Impact Report: Mitigating a Rapidly Emerging Driver of Fraud, accessed July 8, 2013, www.javelinstrategy.com/brochure/287#DownloadReport.

© 2013 Robert Y. Oikawa. Printed with permission.



DR. OIKAWA specializes in HIPAA security, privacy, and Health IT safety coaching. He graduated from the University of Michigan, received his MD and MPH

from Johns Hopkins University, trained as a biomedical engineer, and has practiced as an interventional cardiologist. For the past 15 years, he has focused on information security risk management at Microsoft and MSNBC, and currently as an independent consultant. He may be reached at oikawa@msn.com.

Learn More About HIPAA's Final Rule

FOR FREE

Physicians Insurance CME
www.phyins.com/mycme

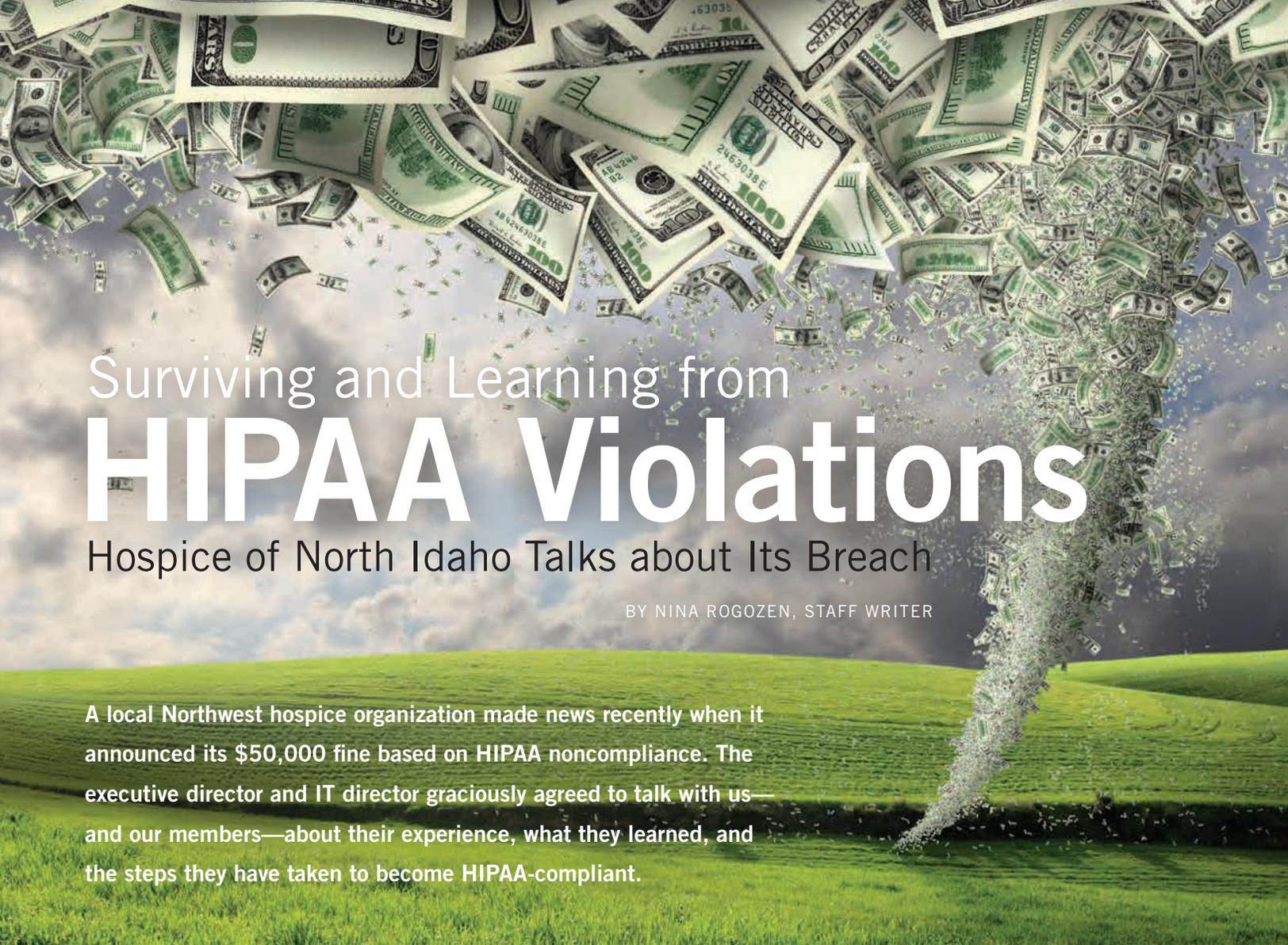
- Understanding the Final HIPAA/HITECH Rules—new in 2013
- Safe and Secure: Medical Office Staff and Patient Privacy
- The Electronic Age: Medical Records, Communication, and Office Policies
- Risk Analysis of PHI Related to Stage II Meaningful Use

Workgroup for Electronic Data Interchange (WEDI)
www.wedi.org

- HIPAA/HITECH Final Rule Summer Webinar Series

FOR A FEE

Nonmembers of Physicians Insurance can now purchase and enroll in our live and online courses at www.phyins.com/store.



Surviving and Learning from HIPAA Violations

Hospice of North Idaho Talks about Its Breach

BY NINA ROGOZEN, STAFF WRITER

A local Northwest hospice organization made news recently when it announced its \$50,000 fine based on HIPAA noncompliance. The executive director and IT director graciously agreed to talk with us—and our members—about their experience, what they learned, and the steps they have taken to become HIPAA-compliant.

Despite a small-town hospice's reputation for providing thoughtful, compassionate, and patient-centered care, something went terribly wrong in June 2010. The U.S. Health and Human Services' (HHS) accusation of HIPAA violations tossed the clinic into a tornado of serious business challenges, a hefty \$50,000 fine, and a time-intensive HIPAA-compliance overhaul.

Hospice of North Idaho (HONI), established in 1981, is a nonprofit, Medicare-certified facility in the small town of Hayden, Idaho. A team of medical providers, volunteers, therapists, dietitians, social workers, and grief counselors care for terminally ill patients and their families. They skillfully attend to patients in their homes or at Hospice House, HONI's 12-room, inpatient facility. However, by the time the Office for Civil Rights (OCR), the HIPAA enforcement arm of HHS, finished its investigation, it was clear that HONI's day-to-day operations would need its own intensive care.

It Only Took an Instant

Shockingly, the seed of HONI's OCR trouble sprouted in about 45 seconds—just long enough for a thief to take off with a hospice worker's laptop from her locked car. The laptop contained unencrypted electronic protected health information (ePHI) of 441 hospice patients. In addition to compromised personal health information, identity theft was now also a huge risk for these patients. "We can provide free credit card monitoring for one year," says Sue Howlett, HONI's Director of IT, who began working at HONI after the breach occurred, "but a social security number is yours for life." Luckily, there has been no indication of foul play and no sign that patients have been affected by the theft.

Why would the theft of a laptop from a locked car, with no indication of negative impact to patients, lead to a hefty \$50,000 fine? The answer comes in layers. The first is HONI's failure to encrypt the electronic files, which would have given them a fortress of protection by keeping unauthorized



Photos courtesy of Hospice of North Idaho

people out. The OCR investigation found that HONI, having no designated Privacy and Security Officer, had not conducted a mandated risk analysis to determine what steps were necessary to secure their patients' PHI. HONI did not evaluate the likelihood of a theft happening or the potential confidentiality risks. In addition, they did not have in place policies and procedures to address mobile device security as required by the HIPAA Security Rule. All of these OCR findings were significant HIPAA violations.

Unfortunately, these oversights can happen even in well-organized, conscientious facilities. Additionally, due to resource constraints, they had outsourced their IT functions to a company that did not regularly deal with HIPAA regulations.

Taking Responsibility, Facing the Fine

When HHS finally determined the \$50,000 fine, it was HONI that sent a press release to the local newspaper. When it landed on the front page, the local community was enraged that their small, local hospice resource was handed such a seemingly large fine. This outpouring of support bolstered

HONI's resolve. They had erred, and the fine illuminated their omissions, but they were taking steps to make things right. Management and staff embraced the challenge of business realignment and made major changes in both their practices and their culture.

Bravely Taking on the Challenge

In 2011, after the data breach, Kim Ransier became executive director. With solid operations experience under her belt, she and the staff began their incredible journey, making it possible for HONI to become a secure, HIPAA-compliant hospice center. When asked what propelled everyone at HONI forward, Ransier's answer was simple—*"Our mission: With open hearts and expertise, we serve the seriously ill and those touched by loss, regardless of their ability to pay."*

Driven by this strong sense of mission, HONI recovered by making difficult business decisions and answering critical questions: How would they pay this hefty fine? How would they develop the new skills they needed? How could they restructure in order to hire in-house IT expertise? Should management lay off individuals or

maintain staffing levels? Should they cut, keep, or suspend vital programs?

"Our staff is the best on the planet," Ransier believes. Despite these significant business challenges, she said, "there was never a question of closing our doors. The \$50,000 fine was a significant chunk of our annual operating revenue. We had to use funds from our annual fund-raisers to offset the expense, which delayed our Kids Bereavement Camp for at least a year." Restructuring meant hiring in-house expertise to implement and maintain HIPAA-compliance measures. That is when they brought in Sue Howlett as director of IT.

When Howlett began at HONI, she started making changes, mindfully correcting the HIPAA violations that led to their \$50,000 fine. Her first main function was getting the agency into compliance. Her logical steps are a good blueprint for action: Howlett conducted a thorough risk analysis and planned to routinely conduct them from then on. HONI now uses a new software program with encrypted files that reinforces HIPAA's security and privacy rules. Their increased security measures include both their mobile and stationary

equipment. Their security policies and procedures are stronger, including robust password enforcement.

“Part of my thinking and job as a leader is to constantly reinforce the importance of the HIPAA regulations with our staff, board, and volunteers,” says Howlett. She conducts staff trainings, presents updates at staff meetings, and sends out periodic security alerts. “It’s all part of our daily work now.”

HONI’s recovery has been substantial, and everyone has embraced the importance of their own compliance obligations. “Our director of IT is on top of these issues,” says Ransier. “We keep this process in the forefront of everyone’s mind, so we are prepared for future demands.”

Ransier is very pleased that HONI’s culture has shifted away from “We are small, nobody cares what we do.” Now she says, “Everybody understands the importance of compliance, including our board, whose members have undergone training as well. This experience really brought the center together in a new way. People are less isolated in their area of expertise or job category. Surviving this ordeal gave us a new, common focus, and it has touched every person and how they now do their job.”

See the back cover for a list of resources to help with ongoing HIPAA compliance.

Lessons Learned

Hospice of North Idaho has learned a lot about itself and its role in ensuring that patient information remains private and secure. You can translate these lessons into what works best for your practice or business.

Regulatory Agencies Can Find You

Sticking your head in the sand protects you from nothing. Remember, even if you are a small practice of two-to-four doctors—in a rural corner of a small state or a large metropolis—assumptions like “HHS doesn’t care about a little group like ours; they go after the big fish” make you vulnerable. HONI’s investigation took place after a routine annual reporting of breaches involving fewer than 500 patients.

Acceptance Takes the Sting Out

“You can’t argue with the findings,” says Howlett. “There are no second opinions.” It is like being caught speeding, except the fine is much, much bigger. In addition to an HHS fine, you will be subject to ongoing monitoring to prove that your organization is making efforts to comply.

Don’t Dread It, Get Ahead of It

Most practices, agencies, and companies dread audits—and investigations even more. Do not wait for an unsuccessful audit to motivate you. By proactively conducting the business of medical privacy, you free yourself up to do what you most want to do—provide high-quality care to your patients. Begin with a structured risk assessment, and make changes from there.

Hire or Delegate Responsibility

“Doctors don’t go to medical school to learn this stuff; they studied to learn how to care for patients,” Howlett points out. So designate or hire someone to fulfill risk-assessment duties and oversee HIPAA compliance. You must bring HIPAA regulations to life, rather than keeping them in a filing cabinet or saving them, unread, on your computer.

Educate Yourself and Your Staff

An OCR pilot auditing project found that the most common cause of deficiency was not knowing HIPAA’s requirements. Empower yourself and your whole team, including your colleagues, with education and training. *Everyone* has a role in the process, and the Final Rule requires that all staff receive training on compliance protocols.

Be a Watchful Hawk

Before outsourcing to an IT company or any other external resource that has access to PHI, verify their HIPAA know-how and complete a Business Associate Agreement with them. While a BA can be fined for HIPAA violations, remember that whenever you outsource, you are still responsible to HHS for HIPAA compliance regarding your patients’ PHI.





HIPAA Q&A

WITH EXPERT LESLIE
MESEROLE, JD

Compliance, Documentation, and Changes Associated with the HIPAA Final Rule

BY NINA ROGOZEN, STAFF WRITER



Leslie is a principal in the health care practice team of Riddell Williams P.S. She has experience working with hospitals and health systems, physicians and physician groups, public hospital districts, and other health care-related entities in business transactions and regulatory compliance matters. Leslie's regulatory compliance practice focuses on fraud and abuse, HIPAA compliance and patient privacy, IRS rules applicable to exempt organizations, physician compensation, and Medicare participation and reimbursement.

Q Documentation seems to be the backbone of compliance, proof that you are acting in accordance with HIPAA regulations. What are some examples of required documentation?

A HIPAA Privacy, Security, and Breach Notification Rules all require extensive written or electronic documentation and retention of that documentation,

generally for six years. A **Covered Entity (CE)**, such as a medical practice or hospital, must document its policies and procedures that demonstrate operational compliance with the Privacy and Security Rules. All compliance-related activities required by the Security Rule must also be documented—for example, risk analysis and risk management programs must document the CE's analysis and management

of risks that **electronic Protected Health Information (ePHI)** could be inappropriately accessed or disclosed. Another example is the technical and physical safeguards a CE establishes to protect the security and integrity of **ePHI**. All of this documentation must be made available to those responsible for implementing the procedures as well as to the U.S. Department of **Health and Human Services (HHS)**, if and when HHS requests it.

CEs must also document their activities and communications with patients, such as Notice of Privacy Practices, records of complaints and resolution, and records related to a patient's right to access and amend the patient's records and to receive an accounting of all disclosures of the patient's PHI. The CE must also document a patient's authorization for use and disclosure of the patient's PHI.

Q What is one of the biggest challenges CEs face regarding documentation?

A One of the more difficult challenges for entities is to actually carry out their day-to-day operations consistently with their policies and procedures. The most significant way of knowing you are in compliance is to conduct an internal audit, which will not only verify sufficient documentation, but also help you identify any gaps between actual practices and the corresponding policies and procedures that need further alignment. Keep in mind, HHS can do an audit of your compliance program and documentation at any time, without much notice.

Q These new mandates make documentation even more important. Do health care entities generally have protocols to comply with required documentation?

A Yes. Most health care providers have documented HIPAA compliance programs that incorporate the administrative, technical, and physical safeguards required by HIPAA. They also include the documents and forms needed to document the CE's communications with patients. The OCR Web site contains some sample forms and educational guidance. You will also find helpful FAQs and a variety of

tips and tools. One example is a December 2012 initiative on methods and tools health care providers can use to protect and secure ePHI when using mobile devices.

Q Are documentation challenges harder or easier, less or more complicated, in clinics and small practices than in larger organizations, e.g., hospitals and HMOs?

A Smaller organizations often have fewer human and financial resources, such as a minimal IT budget, which can make HIPAA compliance a challenge. On the flip side, large organizations have a larger workforce that needs to be communicated with, trained, and monitored, and a greater universe of data (due to high patient volume and a greater range of services) and physical assets that need to be secured, e.g., computers, work stations, and filing cabinets.

Q How would a CE approach documenting its compliance with HIPAA regulations and who would take the lead?

A The CE's Privacy Officer or Security Officer (can be one and the same) is responsible for this. They would also be the focal

point in the event of an investigation or audit. Key components might include privacy and security policies and procedures, forms, having business associate agreements in place, and documentation of workforce training.

Q Any final advice to our members?

A Although HIPAA audit and enforcement activities are on the increase, most practices and facilities have already established strong compliance programs. And even though the March 2013 Final Rule implemented some major changes to HIPAA, the core requirements are largely unchanged. This means that practices and facilities will need to update their programs to implement those changes, but doing so is not a daunting task—approach it by identifying the needed changes and updating only those affected portions of your compliance programs using your already established structure. Physicians Insurance has identified these changes and provided guidance on updating your programs—see the Web site HIPAA page at www.phyins.com/hipaa.

Visit www.phyins.com/Summer2013 to see more HIPAA Q&A topics.

“This final omnibus rule marks the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented. These changes not only greatly enhance a patient's privacy rights and protections, but also strengthen the ability of my office to vigorously enforce the HIPAA privacy and security protections, regardless of whether the information is being held by a health plan, a health care provider, or one of their business associates.”

LEON RODRIQUEZ, DIRECTOR, HHS OFFICE FOR CIVIL RIGHTS



SOCIAL MEDIA MARKETING

Promoting Yourself, Your Practice, or Your Thought Leadership While Staying HIPAA-compliant

BY DAVID KINARD, M.ED.

Many physicians and clinic administrators choose not to promote their practices because of potential HIPAA violations. And the notion of using social media to engage with their community is out of the question because there are too many inherent problems. But what if you could engage with your patient community, promote your practice, and remain HIPAA-compliant—all with your current resources?

According to the Federal Register, the general definition of marketing under HIPAA is a communication about a product or service that encourages recipients to purchase or use the product or service (of the covered entity or third party) in which the intent of the communication is not relevant (67 F.R. 53,186). Most people stop there, but doing so limits your ability to connect and engage with your communities. Promoting health in a general manner is not marketing. Mailings promoting health fairs or support groups, providing information about new diagnostic tools, reminding women to get annual mammograms (67 F.R. 53,189)—all these are completely allowable under HIPAA.

HIPAA does not distinguish between the various marketing channels in its general definition, allowing you to choose the best medium for communicating and engaging with your target population. And while there are some exceptions to the general rule, for the most part you can avoid the more complex and riskier parts of marketing under HIPAA by keeping a few things in mind:

- 1. Become the leading voice** in your community about your field or specialty. Become the clinic or physician that promotes general information and education about a topic—and you can do this via all forms of marketing and social media.
- 2. Always maintain your professionalism** when using social media. Don't use your personal Facebook page for your practice. Instead, start a separate page for your practice or clinic where business information can be posted without your personal photos or family messages getting mixed up.
- 3. Avoid providing** any form of medical care in social media. If a patient asks for help in your Facebook page or via Twitter, simply reply by asking the patient to call the office or make an appointment.
- 4. Never use personally identifiable information** in any of your promotional or social media communications.
- 5. You can use a testimonial** or photo of a patient only if you have a signed release allowing you to do so. Keep in mind that a patient can, at any time, revoke the rights to use his or her image, name, or testimonial, so you will need to create a mechanism to pull materials in circulation if needed.

Marketing and engaging in social media is absolutely allowed under HIPAA. Don't miss out on the opportunity to promote yourself, your practice, or your thought leadership—all while promoting ideas and behaviors that lead to healthier patients. With a little time, and some thoughtful approaches, you can safely market and use social media without running into compliance issues.

Example of how to market your practice and engage in social media—all while being HIPAA-compliant.

-  Post a recipe for two healthy meals on your practice Web site.
-  On your business Twitter account, tweet a link to the recipes on your Web site for healthy eating that week.
-  Post a blog entry on the value of proper nutrition in your diet, highlighting a seasonal food and referencing the recipe you tweeted earlier in the week. Tweet the link to your blog entry.
-  Add a post to your Facebook account highlighting the recipes—inviting people to make the food, take pictures, and post suggestions for improvements.
-  Check Facebook for recipe entries, respond with thanks, and answer questions. Post a 500-calorie-burning activity for the weekend, and ask people to post photos with comments.
-   Rest
-  Review prior week's Facebook posts and respond. Start with a new tweet and repeat the cycle.



DAVID KINARD is Associate Vice President of Marketing and Communications at Physicians Insurance and the past president of the Puget Sound chapter of the American Marketing Association. He is probably tweeting right now about how much he loves his work.

Boost Your Clinic's HIPAA I.Q.

Enroll in Physicians Insurance's New Online Self-Study Course—free to all members

In a recent survey by the Office for Civil Rights (OCR, the enforcer of all things HIPAA), it was discovered that the most common reason for HIPAA deficiencies was lack of knowledge about the requirements.

Always eager to fill a knowledge gap and reduce member risk, the Risk Management team at Physicians Insurance has developed a course to help you and your staff understand what you need to know to be prepared for the September 23, 2013, deadline.

**This course is intended to be risk management advice. Any legal questions should be directed to an attorney.*

Safeguarding Your Practice: Understanding the Final HIPAA/HITECH Rules

This one-hour online self-study course is designed to provide critical information to help members become and remain HIPAA-compliant.*

Geared to all specialties, this course will allow you and your staff to review the course materials at your own pace, and complete an interactive quiz that reinforces key topics discussed throughout the program. The course includes a review and discussion of the final regulations released in January 2013 and covers:

- The HIPAA Privacy Rule
- The HIPAA Security Rule
- The HIPAA Enforcement Rule
- The HITECH Act and the Breach Notification Rule

You will come away understanding what is and is not a “breach” of unsecured protected health information (PHI), the required changes to existing Notice of Privacy Practices, the expanded definition and the documentation rules of working with a “Business Associate,” and topics such as marketing and fundraising under the new HIPAA rules.

WHO SHOULD TAKE THIS COURSE

This course focuses on the 2013 HIPAA Omnibus Final Rule and is relevant to every member of your practice, especially your Privacy and Security Officers who have key responsibilities for helping your clinic achieve compliance by the September 23 deadline.

You can find “Safeguarding Your Practice: Understanding the Final HIPAA/HITECH Rules” by logging into the Physicians Insurance Web site at www.phyins.com/cme/online-courses.



95

Percentage of practitioners in the OCR's 2012 Pilot Audit Program that had at least one HIPAA misstep

LACK OF KNOWLEDGE

#1 reason for HIPAA deficiencies, as cited by the OCR in their 2012 Pilot Audit Program

Live Risk Management WEBINAR



Social Media Patient Engagement & Professional Risks

Many physicians and clinic administrators choose not to promote their practices because they are concerned about potential HIPAA violations regarding professional conduct. And the notion of using social media to engage with their community is out of the question because there are too many inherent problems. But what if you could engage with your patient community, promote your practice, and remain HIPAA-compliant—all with your current resources?

This live, one-hour webinar brings together experts in social media marketing and medical risk management to discuss ways to engage with patients and your community while minimizing your professional risk. You'll learn real-world engagement strategies that don't take a lot of time, and the professional principles you need to protect your practice and patients.

To join us, visit www.phyins.com/SocialMediaWebinar and follow the registration steps.

LAWS IN EFFECT JULY 1, 2013

Hello Medical Assistants, Goodbye Health Care Assistants

Washington Law, Chapter 18.360 RCW

In March 2012 Engrossed Substitute Senate Bill 6237 was passed, creating the new medical assistant (MA) profession and phasing out the health care assistant profession.

Do credentialed health care assistants need a new medical assistant credential? Not if their health care assistant credential is active on the effective date (July 1, 2013) of the new medical assistant law. Those who hold an active, current health care assistant credential will become medical assistants.

If an employee is called a "medical assistant" but does not have a credential from the Department of Health (DOH), will he or she automatically become a medical assistant? No. If your employee does not have an active health care assistant credential before July 1, 2013, but is completing duties outlined in RCW 18.360.050, the employee must meet the minimum requirements currently being set in the rule to apply for and receive a medical assistant credential.

Please check out our summary of the medical assistant rules and regulations at www.phyins.com/risk-management/health-care-assistants. If you have questions, please call Risk Management at (206) 343-7300.

Washington State Department of Health Increases Fee for Copying Records

WAC 246-08-400

Effective July 1, 2013, through June 30, 2015, the maximum allowable charge for copying medical records is:

- **\$1.09 per page** for the first 30 pages • **\$0.82 per page** thereafter
- A \$24 clerical searching and handling fee may be charged under state law, but federal law prohibits charging this fee to the patient or to someone authorized to make health care decisions on behalf of the patient.

The amount you charge for reproducing a record must be limited to your actual cost and may not exceed the maximum allowable charges outlined above. Additionally, Washington State requires that you collect sales tax when charging for medical record copies. You may determine the applicable tax rate for your location using this link to the Washington State Department of Revenue (DOR) Web site: <http://dor.wa.gov/content/findtaxesandrates>.

What's the Fix?

Real-life
HIPAA
Compliance
Issues and
How They
Were
Resolved



The following are real scenarios taken from the Office for Civil Rights Web site. To see more examples of scenarios, visit www.hhs.gov/ocr and search the site for “HIPAA case examples” to view cases organized by issue and covered entity type.

PRIVATE PRACTICE IMPLEMENTS SAFEGUARDS FOR WAITING ROOMS

COVERED ENTITY: Private Practice
ISSUE: Safeguards; Impermissible Uses and Disclosures

A staff member of a medical practice discussed HIV testing procedures

with a patient in the waiting room, thereby disclosing PHI to several other individuals. Also, computer screens displaying patient information were easily visible to patients. Among other corrective actions to resolve the specific issues in the case, OCR required the provider to develop and implement policies and procedures regarding appropriate administrative and physical safeguards related to the communication of PHI. The practice trained all staff on the newly developed policies and procedures. In addition, OCR required the practice to reposition its computer monitors to prevent patients from viewing information on

the screens, and the practice installed computer monitor privacy screens to prevent impermissible disclosures.

PRIVATE PRACTICE REVISES PROCESS TO PROVIDE ACCESS TO RECORDS REGARDLESS OF PAYMENT SOURCE

COVERED ENTITY: Private Practice
ISSUE: Access

At the direction of an insurance company that had requested an independent medical exam of an individual, a private medical practice denied the individual a copy of the

medical records. OCR determined that the private practice denied the individual access to records to which she was entitled by the Privacy Rule. Among other corrective actions to resolve the specific issues in the case, OCR required that the private practice revise its policies and procedures regarding access requests to reflect the individual's right of access regardless of payment source.

HOSPITAL IMPLEMENTS NEW MINIMUM NECESSARY POLICES FOR TELEPHONE MESSAGES

COVERED ENTITY: General Hospital
ISSUE: Minimum Necessary; Confidential Communications

A hospital employee did not observe minimum necessary requirements when she left a telephone message with the daughter of a patient that detailed both her medical condition and treatment plan. An OCR investigation also indicated that the confidential communications requirements were not followed, as the employee left the message at the patient's home telephone number, despite the patient's instructions to contact her through her work number. To resolve the issues in this case, the hospital developed and implemented several new procedures. One addressed the issue of minimum necessary information in telephone message content. Employees were trained to provide only the minimum necessary information in messages and were given specific direction as to what information could be left in a message. Employees also were trained to review registration information for patient contact directives regarding leaving messages. The new procedures were incorporated into the standard staff privacy training, both as part of a refresher series and mandatory yearly compliance training.

CLINIC SANCTIONS SUPERVISOR FOR ACCESSING EMPLOYEE MEDICAL RECORD

COVERED ENTITY: Outpatient Facility
ISSUE: Impermissible Use and Disclosure

A hospital employee's supervisor accessed, examined, and disclosed an employee's medical record. OCR's investigation confirmed that the use and disclosure of protected health information by the supervisor was not authorized by the employee and was not otherwise permitted by the Privacy Rule. An employee's medical record is protected by the Privacy Rule, even though employment records held by a covered entity in its role as employer are not. Among other corrective actions to resolve the specific issues in the case, a letter of reprimand was placed in the supervisor's personnel file and the supervisor received additional training about the Privacy Rule. Further, the covered entity counseled the supervisor about appropriate use of the medical information of a subordinate.

PRIVATE PRACTICE PROVIDES ACCESS TO ALL RECORDS, REGARDLESS OF SOURCE

COVERED ENTITY: Private Practice
ISSUE: Access

A private practice denied an individual access to his records on the basis that a portion of the individual's record was created by a physician not associated with the practice. While the amendment provisions of the Privacy Rule permit a covered entity to deny an individual's request for an amendment when the covered entity did not create that portion of the record subject to the request for amendment, no similar provision limits individuals' rights to access their protected health information. Among other steps to resolve the specific issue in this case,

OCR required the private practice to revise its access policy and procedures to affirm that, consistent with the Privacy Rule standards, patients have access to their records regardless of whether another entity created information contained within it.

LARGE HEALTH SYSTEM RESTRICTS PROVIDER'S USE OF PATIENT RECORDS

COVERED ENTITY: Multi-Hospital Health Care Provider
ISSUE: Impermissible Use

A nurse practitioner who has privileges at a multi-hospital health care system and who is part of the system's organized health care arrangement impermissibly accessed the medical records of her ex-husband. In order to resolve this matter to OCR's satisfaction and to prevent a recurrence, the covered entity terminated the nurse practitioner's access to its electronic records system, reported the nurse practitioner's conduct to the appropriate licensing authority, and provided the nurse practitioner with remedial Privacy Rule training.

HIPAA TIP:

Texting patient information? Don't.

Your mobile device might be secure, but how secure is your partner's device? And the networks your message travels through to get there? Since it's hard to know for sure, it's important to exclude patient-specific information of any kind.



For ongoing HIPAA tips, follow us: www.twitter.com/PhysicianInsure.

So Long, But Not Goodbye

We would like to take a moment to thank the 2012 outgoing Board members and friends for their dedication:

Grant E. McLaughlin

James P. Campbell, MD
(Former Chairman)

During their leadership tenure, Physicians Insurance significantly increased its financial strength and delivered a consistent dividend to our members. As Directors, they supported and encouraged a dramatic expansion of the company's risk management offerings, including specialty-specific services, a Medicine in the Courtroom pilot program for third-year residents, and simulation-style CME. They provided leadership as the company strengthened its strategic planning process, acquired EMPAC and SCRUBS RRG management companies, and expanded its ability to provide insurance and services to large health care systems and their physicians.

Jim and Grant will be greatly missed but not forgotten. They are immensely talented and wholly committed to the mission and vision of Physicians Insurance. Board service is a privilege and a serious responsibility. Both have been outstanding in the performance of their responsibilities and it has been an honor to have worked with them!

NEW 2013 Board Members Ready to Serve!

Physicians Insurance is lucky to have a pool of talented and involved Board members. At the spring 2013 annual meeting, the members elected two new Directors whose profiles are provided below. They have been elected to three-year terms of office, and we look forward to their ongoing support and guidance.

APARNA ANANTH, MD



Seth GS Medical College and KEM Hospital, Bombay, India, MBBS (2001); Henry Ford Hospital, Detroit, Michigan, Residency in Anesthesia (2002–2006); University of Washington, Fellowship in Cardiothoracic Anesthesiology (2006–2007)

BOARD CERTIFIED: Anesthesiology and Perioperative Transesophageal

Echocardiography

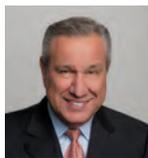
PRESENT POSITION: Practicing Anesthesiologist, Pacific Anesthesia, St. Joseph Medical Center (2012–present)

PRACTICE LOCATION: Tacoma, WA

PROFESSIONAL APPOINTMENTS: Member, American Society of Anesthesiologists, House of Delegates (June 2012–present); Member, Committee on Practice Management, American Society of Anesthesiologists (Oct 2010–present); Member, Committee on Cardiovascular and Thoracic Anesthesia, American Society of Anesthesiologists (Oct 2010–present); Member, Board of Trustees, Washington State Medical Association (Sept 2011–present); Director, Washington State Society of Anesthesiologists (2009–present); Insured by Physicians Insurance since 2007

COMMITTEE: Risk Management/Education

JOHN PASQUALETTO



California State University, Northridge, BA (1965)

PRESENT POSITION: Retired

PAST POSITIONS: President, Chairman, and CEO, Seabright Holdings (SBX, a New York Stock Exchange publicly traded company); CEO and Chairman of SeaBright Insurance Company

and Paladin Managed Care Services and Chairman of PointSure Insurance Services (all subsidiaries of SBX); Senior Vice President, Kemper Insurance Companies; President, CEO, and Director of Eagle Insurance Group; Co-Founder, President, CEO, and Director of Great States Insurance Company

PROFESSIONAL SOCIETIES/AFFILIATIONS: Chairman of California Workers' Compensation Institute; Board Member of the Integrated Benefits Institute; Board Member of NCCI Holding and Chair of its Audit Committee

WELCOME TO OUR NEW MEMBERS!

PROFESSIONAL LIABILITY COVERAGE

Active Family Healthcare
Hayden, ID

Advanced Family Medicine
Kuna, ID

Amercho Medical Specialty Clinic
Bellevue, WA

Bellingham Arthritis & Rheumatology Center
Bellingham, WA

Benson Medical Group
Mount Vernon, WA

Coast to Coast Health Care
Kellogg, ID

Garden City Community Clinic
Garden City, ID

GreenField Health
Portland, OR

Issaquah Obstetrics & Gynecology
Issaquah, WA

Laser Treatment Center
Kirkland, WA

Northwest Cancer Clinic
Kennewick, WA

Oregon Orthopedic & Sports Medicine Clinic
Oregon City, OR

Pacific Pathology Partners
Seattle, WA

Pinnacle Pain Center
Kennewick, WA

Portland Diabetes & Endocrinology Center
Portland, OR

Sunnyside Community Hospital
Sunnyside, WA

St. Mark's Eye Institute
Tacoma, WA

The Dermatology Clinic
Mercer Island, WA

The Wellness Tree Community Clinic
Twin Falls, ID

Urocare
Twin Falls, ID

Vera Whole Health
Seattle, WA

Willamette Valley Cancer Institute & Research Center
Eugene, OR

PROVIDER EXCESS & REINSURANCE

Trillium Community Health Plan
Eugene, OR

MEDICAL STOP-LOSS

CellNetix Pathology
Seattle, WA

Lake Chelan Community Hospital
Chelan, WA

Olympia Orthopaedic Associates
Olympia, WA

Reelected to new three-year terms of office were the following incumbent Directors.

SHEILA REGE, MD



University of California, Berkeley, BS (1985)

University of California, Los Angeles, School of Medicine, MD (1989)

University of California, Los Angeles, Residency in General Surgery (1991), Nuclear Medicine (1993), and Radiation Oncology (1997)

BOARD CERTIFIED: Radiation Oncology
PRESENT POSITION: Radiation Oncologist, Northwest Cancer Clinic
PRACTICE LOCATION: Tri-Cities, WA
PROFESSIONAL APPOINTMENTS: AMA Alternate Delegate (2008-present), Chair of BFCMS Technology/IT Committee (2007–2008), Center for

Health Care Reform Advisory Board, WA Policy Center (2006–present), Member of ASTRO Government Relations Congressional Relations Subcommittee (2005–present), Board Member, American College of Radiation Oncology Insured by Physicians Insurance since 1997

COMMITTEES: Underwriting/Sales/Marketing and Internal Nominating Incumbent; first elected in 2010

COMMITTEES: Executive, Finance & Audit, Investment, and Compensation Incumbent; first elected in 2010

COMMITTEES: Executive, Finance & Audit, Investment, and Compensation Incumbent; first elected in 2010

COMMITTEES: Executive, Finance & Audit, Investment, and Compensation Incumbent; first elected in 2010

COMMITTEES: Executive, Finance & Audit, Investment, and Compensation Incumbent; first elected in 2010

RALPH ROSSI, MD



Yale College, BA (1984)

University of California, San Diego, MD (1991)

University of Washington, Residency in Internal Medicine (1991–1994)

University of Washington, MPH (1997)

University of Washington, MPH (1997)

BOARD CERTIFIED: Internal Medicine

PRESENT POSITION: Practicing physician; Immediate Past President, Chair, Finance and Operations Committee, and member, Strategic Planning Committee at The Polyclinic

PRACTICE LOCATION: Seattle, Washington

COMMITTEES: Executive, Finance & Audit, Investment, and Compensation Incumbent; first elected in 2010

COMMITTEES: Executive, Finance & Audit, Investment, and Compensation Incumbent; first elected in 2010

COMMITTEES: Executive, Finance & Audit, Investment, and Compensation Incumbent; first elected in 2010

TELL US WHAT YOU THINK!

We're eager to hear member feedback. Please let us know what you think of our new format and what you'd like to see in future issues at editor@phyins.com.

Hey, Cancer: Consider Yourself Warned



Dr. Bill Winter on his Fender Stratocaster, performing with N.E.D. (No Evidence of Disease)

When discussing cancer, it's not common for the conversation to wind up covering Hula-Hoop skills, live Hawaiian music, stand-up comedy, and rock bands. But when you spend a few minutes with Bradley Perrigo from Compass Oncology, you find that these topics (and more) are pretty familiar to his team.

As a cancer care practice with an interdisciplinary approach, Compass Oncology's seven sites offer a full team of physicians—oncologists, hematologists, radiation oncologists, breast and gynecologic oncology surgeons, pathologists, PAs, and more—all focused on helping patients and families as they journey through the maze of cancer treatments. And though they are the last non-hospital-owned cancer care practice in the Portland-Vancouver metro area, that's not what they might say makes them unique. According to Brad, it's the staff: "They're driven and ambitious, whether at work or at play."

Compass Oncology Isn't Playing Around

It certainly takes a special type of professional to help patients deal with the highs and lows of cancer care today: the high costs of cancer drugs, low Medicare reimbursements, finding economic resources for the uninsured and underinsured, and the exciting yet challenging aspects of oral chemotherapy—to name a few. For Brad, working with the people at his practice is his favorite part of the job, due to their compassion for families and patients. Though a cancer diagnosis is not always the death sentence it used to be, the staff is tasked daily with teaching patients about living life with a new idea of normal—even if they go about it in a non-normal sort of way.

"At summer events, we used to put our physicians in the dunk tank to help raise money for patients needing extra help," says Perrigo. "Today, on a daily basis, patients love to hear our nurses laughing as they go about their work," says Perrigo. "And the patients themselves start laughing when the nurses put on their gowns and gloves to pump the chemotherapy. The nurses kind of look like Smurfs."

There is something special about oncologists. They have an insatiable desire to keep going, keep researching, and keep learning—all because they want a better outcome for the patient. They are tireless and driven, yet tender and compassionate.

They're also the kind of people whose idea of letting their hair down at the annual holiday party involves not just a talent show, but a competitive event for charity. That's where Brad finds out about his staff's hidden talents. "One supervisor is incredible with a Hula-Hoop, a radiation therapist does a terrific Andy Williams impersonation, and one of our pathologists moonlights in a Hawaiian music band (and he's not even Hawaiian)!"

And if you watched *TODAY* last September, you might have seen and heard Dr. Winter and his rock band

Fast Facts

ESTABLISHED: 1976

LOCATION: 7 locations throughout Oregon and SW Washington

TOTAL STAFF: 300 employees, 42 physicians

PHYSICIANS INSURANCE MEMBER: Since 2010



The Compass Oncology West crew at the 2012 Race for the Cure: Korrina Gonzales, Brenda Brua, Kirk Stewart, Karen Adetunji, Sophear Yim, Julie Short, Erin Isbell, Lucy Langer, and Bonnie Blake-Night

“One of the most exciting aspects of cancer care today? Seeing cancer patients thrive for years as survivors. My mom was diagnosed and treated for cancer in 1982. Today she is a healthy, vibrant woman in her seventies.”



Brad Perrigo
Executive Director
Compass Oncology

N.E.D. (which stands for “No Evidence of Disease”). Members are gynecologic oncologists performing original music to empower women stricken by cancer.

Suffice it to say, you don’t have to look hard within Compass Oncology’s nearly 350 staff and physicians to find talented, driven, mission-focused professionals. That’s pretty typical of Physicians Insurance members, and the Compass crowd is no exception.

Now You Can Get Certificates of Insurance On Demand 24/7

You’ve got a list of physicians whose hospital credentials need updating, and you need COIs fast. Faster than you can dial the 800 number and talk to the good people in the Underwriting Department at Physicians Insurance. Besides, it’s 7 p.m. and you just learned they need to be there by morning.

Physicians Insurance recently launched an online document delivery tool enabling you to search, sort, save, and download Certificates of Insurance (COIs) for all the physicians you manage. A quick search, a few clicks, and a PDF of the certificate you need is at your fingertips for download.

How It Works

Sign in to your Physicians Insurance online account, and select “COI Documents” from the “Your Account” tab. You can search for just one or multiple certificates, using name, policy number, or client ID. Then, when you’re ready, download the resulting PDF and it will appear on your computer in a folder. Multiple certificates can be merged as one, or you can download them as individual files—whatever you need. Searches can be downloaded on the spot, or saved for later if you get interrupted and need to come back.

Super Convenient

Though you can still call our office and request a COI, it’s nice to know you can generate one at any time—even after hours or on the weekends. So when a physician is being credentialed at a new hospital over the weekend, and you need the COI to finalize the process for privileges, or if you don’t quite remember where the COI was filed during the beginning-of-year rush—now you have the ability to generate COIs with just a few clicks of the mouse.

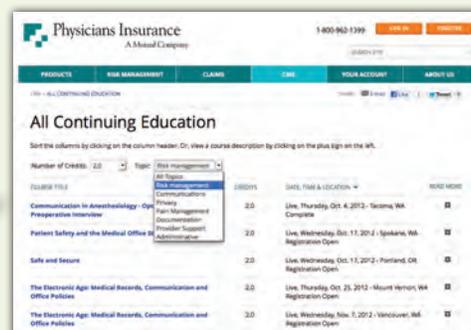
An Online User Account with Physicians Insurance

THE KEY TO ACCESSING A LIBRARY OF ONLINE RESOURCES

You spoke, we listened. You wanted online access to all the great resources we provide with your policy. So we built a password-protected area of our Web site for all members—physicians and staff members alike—to access CME, tools, videos, sample forms, HIPAA resources, online payments, and more. We’re continually adding resources to these members-only pages, such as our new Certificate of Insurance document delivery tool.

To set up your online user account, visit www.phyins.com and select the **CREATE ACCOUNT** button in the upper right corner. Registration takes only three quick steps. You’ll want to have your medical license number or the Physicians Insurance policy number you are associated with when you first set up your account. Then, remember your user name and password for future use.

If you already have an online account and have forgotten your password, select “Recover Password” on the log-in page to trigger an e-mail from Physicians Insurance that allows you to reset your password. If our system does not recognize what you believe is your user name, please contact us at (800) 962-1399.



mandatory arbitrations. This may be viewed as undesirable as the arbitrators may be unknown to the parties or have limited experience in the complexity of medical negligence. However, with limited risk, it allows us to develop the next generation of defense attorneys by giving them experience presenting a case in arbitration.

In the second half of 2012, Physicians Insurance had one case resolved by voluntary arbitration and two cases resolved by mandatory arbitration. A representative example of each follows. Because arbitrations are often private matters, not of public record, we have changed all the details of the cases to maintain anonymity.



“The arbitration process can sometimes offer advantages over a jury trial for all parties. It generally switches the focus from emotion to the facts of a case. It is also less stressful and nonpublic, and it results in faster final resolution.”

Gary Morse, Senior Vice President & General Counsel, Physicians Insurance

A GENERAL SURGERY CASE RESOLVED BY VOLUNTARY ARBITRATION

ALLEGATION: A physician who was not insured with us performed urological surgery on a male patient. Our insured physician was called in to repair a rectal laceration, and he proceeded to repair the rectum and perform a diverting colostomy. Complications from the colostomy resulted in subsequent procedures. The patient claimed \$1 million in damages consisting of medical expenses, pain and suffering, and a failed business.

PLAINTIFF ATTORNEY: Confidential

PLAINTIFF EXPERT: General Surgeon

DEFENSE ATTORNEY: Confidential

DEFENSE EXPERT: General Surgeon

RESULT: Plaintiff verdict for \$59,000,
Retired Superior Court Judge

A RADIOLOGY CASE RESOLVED BY MANDATORY ARBITRATION

ALLEGATION: A patient alleged negligence from a procedure in which a hemothorax is a known complication. Approximately ten days following the procedure, the patient required a thoracentesis. The patient claimed additional medical expenses and pain and suffering, totaling \$50,000.

PLAINTIFF ATTORNEY: Confidential

PLAINTIFF EXPERT: Radiologist

DEFENSE ATTORNEY: Confidential

DEFENSE EXPERT: Radiologist

RESULT: Defense verdict, Private Arbitrator

Read more trial results at www.phyins.com/claims/trial-results.

1301 Second Avenue, Suite 2700
Seattle, WA 98101

THE PHYSICIANS REPORT | SUMMER 2013

RESOURCES to Help with Ongoing HIPAA COMPLIANCE

A number of Web sites provide tools and information on establishing HIPAA-compliance programs. Here is a partial list; some resources are for members only.

- **Physicians Insurance**
www.phyins.com/hipaa
- **American Hospital Association**
www.aha.org/advocacy-issues/hipaa
- **American Medical Association**
www.ama-assn.org/go/hipaa
- **Healthcare Information and Management Systems Society**
www.himss.org
- **American Health Lawyers Association**
www.healthlawyers.org
- **Oregon Medical Association**
www.theoma.org/HIPAA
- **Idaho Medical Association**
www.idmed.org/displaycommon.cfm?an=1&subarticlenbr=94
- **HHS Web site**
Audit protocol and enforcement:
www.hhs.gov/ocr/privacy/hipaa/enforcement/
Case studies:
www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/



HIPAA



Everything else