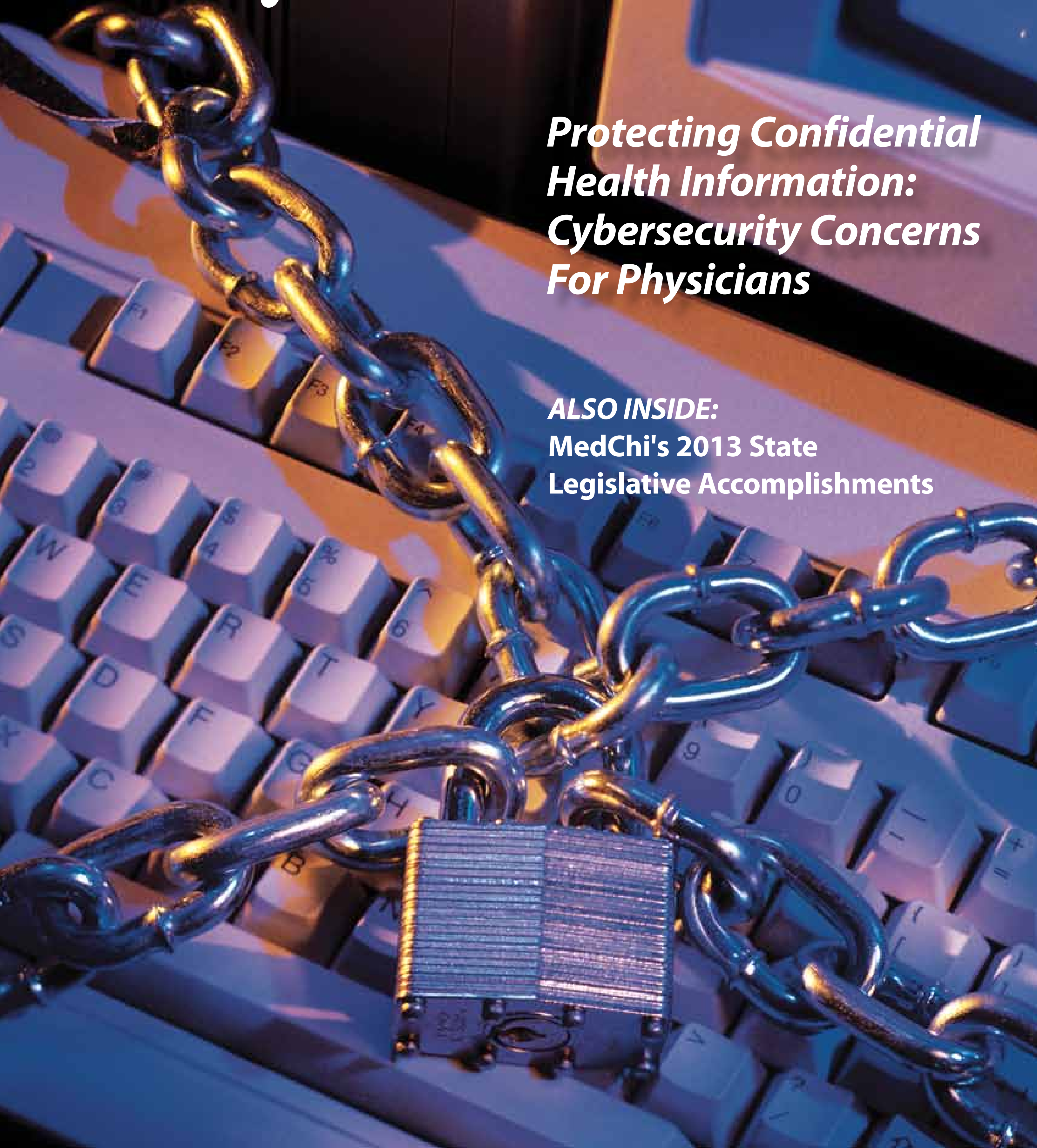
MarylandMedicine

The Maryland Medical Journal Volume 14, Issue 2



Protecting Confidential Health Information: Cybersecurity Concerns For Physicians

ALSO INSIDE:

MedChi's 2013 State Legislative Accomplishments

SURVIVE AND THRIVE
in a Patient-Centered Medical Home model
Q&A with Lew M. Levy, MD

Best Doctors' Vice President of Corporate Medical Quality, Dr. Lewis M. Levy, Instructor in Medicine at Harvard Medical School, explains how the company's consulting services can benefit doctors in the new era of the PCMH.

Q: What is Best Doctors, and how does it support the patient-centered medical home (PCMH)?

A: At Best Doctors, we support treating physicians in finding evidence-based options in diagnosing and treating challenging cases. When a treating physician faces a difficult case, he or she can contact Best Doctors and receive a thoughtful, well-researched opinion from a nationally recognized specialist. This isn't a utilization review; it is a superb resource for doctors who are working on challenging cases.

As the nation's doctors move to the PCMH model, this type of efficient, evidence-based resource will be a powerful way to improve patient outcomes and satisfaction.

Q: How can Best Doctors be a valuable resource for practices using new PCMH payment models?

A: Most PCMHs are using performance based payment models which recognize achievement of care quality and efficiency goals. This includes incentives to identify the right diagnosis and treatment while avoiding extraneous tests and specialty referrals. It also means finding cost-effective ways to care for your complicated, high-cost patients. Best Doctors services are a resource that can help them provide high-quality, evidence-based care and still come in under budget, allowing you to keep more payment incentives.

Q: How can Best Doctors improve on the professional network doctors have already established?

A: Most doctors have an excellent network of colleagues to whom they routinely refer patients. The Best Doctors process provides an expert second opinion, typically in much less time than it takes to schedule an appointment at a specialty or teaching hospital. In addition, Best Doctors often provides treating physicians with a complete and comprehensive clinical history of their patient. It's one way Best Doctors can help support medical practices in providing a better patient experience, which is a key component of becoming and/or maintaining status as a PCMH.

Q: Has Best Doctors seen through their clinical process that collaborative medicine improves diagnosis and treatment?

A: When medical information is organized and physicians work together, the patient benefits and outcomes improve. We've seen this in our global health company for over 20 years.

Q: Why does Best Doctors work to support physicians in this way?

A: We sell our service to large employers and health plans as a part of their employee/member benefits offerings. Our relationship with physicians is never commercial. We are a trusted resource for physicians who are ready for the collaborative future of health care.

Watch our weekly PCMH videocast series for free at **youtube.com/BestDoctorsTV** or download as a free podcast at **bestdoctors.com/PCMH**. Subscribe to this series at **bestdoctors.com/Subscribe.**

Best Doctors®

Best Doctors brings together the best medical minds in the world to help identify right diagnosis and treatment for patients. Our innovative, peer-to-peer consultation service offers a new way for physicians to collaborate with other physicians to help patients. Best Doctors serves nearly 30 million members worldwide, including the US, and is now one of the world's fastest-growing health companies. For further information, visit **www.bestdoctors.com.**

Volume 14 Issue 2

INSIDE

Our managing editor of fourteen years, Susan Raskin, has assumed her new role of full-time grandmother. We will miss her.

Features

Departments

Scan the code with your smart phone and download *Maryland Medicine* to your mobile device.

MedChi's Efforts Paid Off During the Legislative Session!

PRESIDENT'S MESSAGE

Brian H. Avin, MD

This issue of *Maryland Medicine* highlights MedChi, the Maryland State Medical Society's 2013 legislative efforts. I want to recognize the herculean efforts of our advocacy team led by Jay Schwartz, Pam Metz Kasemeyer and Steve Wise. They worked tirelessly during the 2013 legislative session to promote our health care issues with clear, concise positions developed under the direction of the Council on Legislation. In addition our advocacy team represents MedChi throughout the year, serving on task forces and commissions, and attending meetings of committees that develop policies and regulations, a never-ending process.

Other leaders of the team include MedChi's CEO and superstar Gene Ransom, the legislative council chairs James York, MD and Brooke Buckley, MD and subcommittee chairs Gary Pushkin, MD (health insurance), Stephen Rockower, MD (boards and commissions), and James Chesley Jr., MD (public health). Thanks to all the members of the legislative council who gave their time to review more than 250 bills during the session. They offered insight and expertise on a multitude of issues that became MedChi's positions after being approved by the MedChi House of Delegates. We also appreciate the significant grassroots efforts of our component society staff and members.

The mission of MedChi is to serve as Maryland's foremost advocate and resource for physicians, their patients and the public's health. The Society, through its members, lives this mission every single day.

Below are some of the public health initiatives that MedChi has advocated for over the last two years:

- Making texting and the use of hand held cell phones while driving, primary offenses. Hopefully, that will decrease distracted driving and the accidents that accompany their use.
- Preventing those under the age of 18 from using tanning beds. Tanning bed exposure increases the incidence of skin cancer (malignant melanoma, basal and squamous cell). MedChi's prior efforts requiring adolescents to present a letter from a parent or guardian consenting to the use of tanning beds have, ironically, hindered our ability to take this next step.
- Making EpiPens available in public and private schools in order to treat children with life-threatening allergic reactions.
- Placing automated electronic defibrillators in schools, health clubs and large venues (such as malls), thus allowing individuals with life-threatening cardiac arrhythmias a chance to be successfully resuscitated.
- Eliminating arsenic from animal feed. We are now working to have antibiotics removed from animal feed.
- Advocating for increased tobacco taxes that will be used to maintain the integrity of the Medicaid program and ensure that participants have access to physicians.
- Ensuring that Maryland is the only state in the country where Medicaid will pay Medicare rates to ALL Maryland physicians for evaluation and management services. In order to sustain this level of payment, primary care physicians who treat Medicaid patients must submit forms for payment. Forms can be found at dhmh.maryland.gov.
- Requiring all licensed health care practitioners to wear a picture ID with their name and licensing credentials, was the result of our *Truth in Advertising* initiative supported by Attorney General Douglas Gansler. For example, my badge has my mug shot and simply states: *Brian H. Avin, MD, Physician, Neurologist.*
- Establishing *Insurance Watch*, a website where patients, consumers and physicians can download the form developed to file a grievance with the Attorney General's office against insurance companies that deny or obstruct the delivery of health care, or refuse to pay for care. This form is located at medchi.org.
- Sponsoring the free Maryland Prescription Card program that offers individuals who do not have pharmacy coverage or who have high deductible plans, up to a 75 percent discount on prescription drugs. The card can be printed from medchi.org.
- Advocating for healthy meals and increased physical activity in schools, in addition to educating the public on health hazards associated with sugary beverages.
- Establishing three Accountable Care Organizations (ACOs). These are health care delivery systems administered by primary care physicians to better integrate and coordinate care that will improve quality of care and health outcomes, while decreasing health care costs.
- Partnering with clinics being established in Capital Heights, Prince George's County, and in Dorchester and Caroline Counties. These clinics are located in the five Health Enterprise Zones, established by Lieutenant Governor Anthony Brown, and are modeled after Business Enterprise Zones in geographic locations with the worst public outcomes. Physicians who participate with these clinics will receive tax and health information technology incentives.

In an effort to incentivize physicians to use electronic health records, Maryland is the only state in the country that now requires each state-regulated health insurance company (Aetna, CareFirst, Cigna, Coventry, Kaiser and United

continued on page 8

Maryland's Medicare Waiver: Why It Should Matter to You

CEO'S MESSAGE

Gene Ransom, III

Maryland is a unique state when it comes to hospital payments. We are the only state that enjoys a waiver providing over a billion dollars in extra federal funds for hospital facility fees. The federal funds are contingent upon Maryland hitting certain cost measures, or a waiver test. Recently that test has been under pressure, and the state is dangerously close to not making the grade. (See figure at right.) The waiver has been in place since 1971, and because of health system reform, the waiver test pressure and other factors, it is currently up for reconsideration before the state and federal government. MedChi, the Maryland State Medical Society, has been working collaboratively with all physicians and specialty societies to improve the waiver, as it affects physicians greatly.

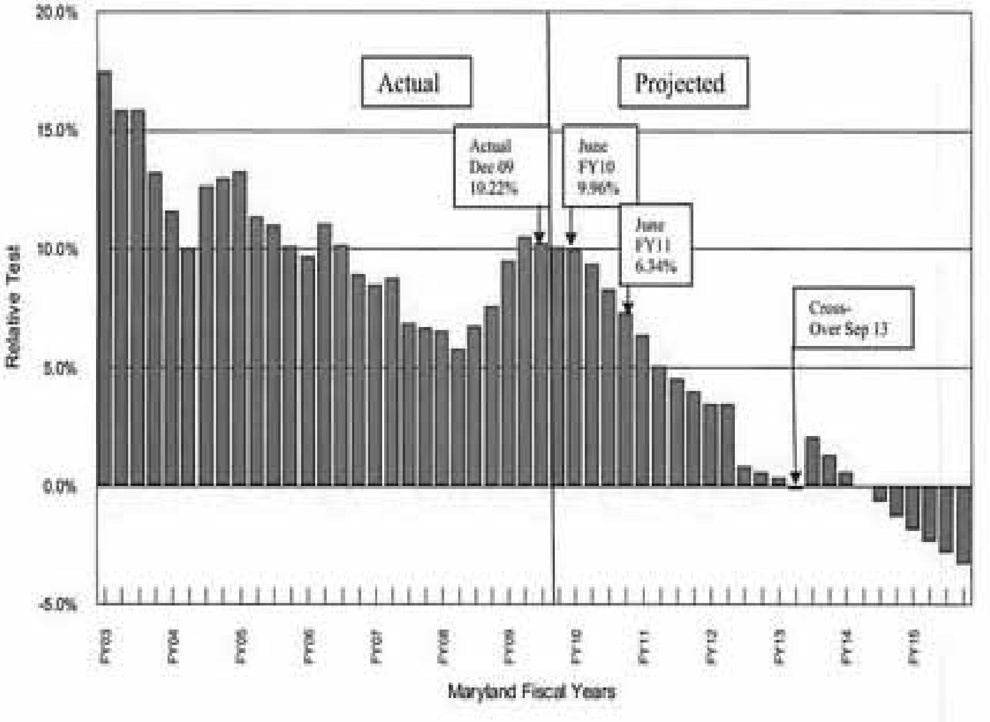
To that end the various physician groups and MedChi understand the need for better management of health care costs, improved quality of care and payment reform. There is no better evidence to demonstrate the physician/MedChi commitment to this cause than the approved Maryland Accountable Care Organizations (ACOs) co-sponsored by MedChi. However, MedChi and the physician community strongly believe that as Maryland moves forward with new payment models and modernizing the waiver, we need to impress upon policymakers the necessity of being careful with any bundled payment programs that affect payments for professional services.

MedChi has been involved in the waiver process and we continue to work to achieve the above goals for Medicine. This is the biggest issue for health care in Maryland and every practicing physician, regardless of where they practice, needs to understand the waiver and what it will mean to their practice.

Gene Ransom, III, CEO of MedChi. His email is gransom@medchi.org, and he may be contacted at 1.800.492.1056. He would like to thank the Maryland legislature for collaborating with MedChi to help physicians and hospitals receive payment for services rendered.

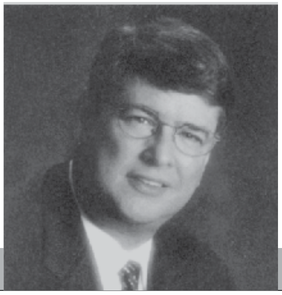
Actual and Forecasted Waiver Cushions FY 2003-FY2015

Medicare Waiver Cushion



Organized medicine has recommended the following principles with regard to bundled payment programs in Maryland:

- Inclusion of gain sharing with physicians as a new tool for facility fee bundled payment programs
- Use of measures in the waiver that ease and increase participation in the Medicare ACO program
- Support of new programs and innovations to create incentives to improve Medicaid in the unregulated outpatient system
- Special tort protection granted to physicians in bundled payment models that address the cost and risk of defensive medicine
- Not implementing bundled payment programs for professional services as these would create tension between hospitals and physicians, produce negative incentives for the system, increase costs, and generally increase the risk to the waiver.



I Guarantee You

EDITOR'S CORNER

Bruce M. Smoller, MD

I am in Chicago, attending the annual AMA convention in this city of great architecture, food, hockey and medicine, and I am impressed. By Chicago, this city of my birth, and its direct, palpable, earthy presence, surely. By the incredibly well run and actually meaningful business of the AMA, and the commitment of the people here, definitely.

I am most impressed, however, with our students and residents. I am absolutely and very pleasantly astounded to learn that there are over 15 medical students from Maryland here at the AMA as accredited representatives, and that's just from Maryland. I am told that MedChi, the Maryland State Medical Society, and particularly CEO Gene Ransom, have been as welcoming as possible to these students and that there is among them, back at Hopkins, a mentor who believes that they should be a part of their AMA in person as well as back home.

These students are as committed, perceptive, engaged and thoughtful a group as I have chanced upon as both a participant in organized medicine and as a clinical professor at George Washington University School of Medicine for 37 years. They have names and faces as diverse as the outside world, and they are our lifeblood, without whom our 214-year-old MedChi and our 166-year-old AMA would fade and wither. They are knowledgeable about many of the issues facing physicians today and they think that they have some answers, or at least they are asking the right questions.

They are also tech savvy. I mean really tech savvy. I sat at a table, with my fingers on a gadget the size of an iPhone without the phone and had my EKG taken, and sent by low frequency sound waves to a smart phone a couple of feet away and read by another medical student who was surprised that we older folk thought this to be the magic of the future arrived now in the present by…well, magic. This is great stuff…and I don't mean just the tech stuff.

The presence of these, and other committed, involved and smart students and residents kind of mutes and puts into perspective some of the fears and struggles of our present concerns. Of course, tort reform, and affordable care, ACOs and SGRs are important…they are very important to the satisfaction of our physician community and, thus, our families and our patients. But we have backup. If we don't prevail now, we have time to prevail later. Not to put too fine a point of popular culture to it, as Yoda and Obi-Won say to each other when despairing about the future of the Jedi, "No, there is another." So, too, can we say that to each other, though that doesn't let us off the hook one bit on the "trying like hell now" gambit.

So to all the MedChi members reading this who know someone who won't join MedChi or the AMA because they think it is not worth it, or because they are sure that organized medicine has done nothing for them and **will** do nothing for them, and, besides, they need a new widget and can't afford to become part of the solution, or who think that the AMA is their enemy and doesn't care about their welfare and satisfaction, I'll skip the hundred and one reasons they are wrong, and skip the homilies about how the AMA isn't "everybody else"– it's **us**, and just point to these students and residents and tell you, straight out, that if they can see the reasons to be so involved, you surely can, and if you can't, move over, 'cause they'll roll right over you on their march to progress, solutions and success. I guarantee you of that.

This issue of *Maryland Medicine*, devoted to cybersecurity, was mostly produced before the public disclosure of great government surveillance programs designed to capture cyber data in the service of national security. We think it is very timely and invite you, our readers, to send us your comments about that and other cybersecurity issues in this time of inflation in the use of electronic health records and computers. Thank you.

EDITORIAL STATEMENT

Editorial Offices
Montgomery County Medical Society
15855 Crabbs Branch Way
Rockville. MD 20855-0689
Phone 301.921.4300, ext. 202
Fax 301.921.4368
ksisson@montgomerymedicine.org

Advertising
800.492.1056

Classified and Display Advertising Rates
Kevin Lyn Sisson
301.921.4300, ext. 202
ksisson@montgomerymedicine.org

All opinions and statements of supposed fact expressed by authors are their own, and not necessarily those of Maryland Medicine or MedChi. The Editorial Board reserves the right to edit all contributions, as well as to reject any material or advertisements submitted.

Copyright © 2013. Maryland Medicine, The Maryland Medical Journal. USPS 332080. ISSN 1538-2656 is published quarterly by the Medical and Chirurgical Faculty of Maryland, 1211 Cathedral Street, Baltimore, Maryland 21201, and is a membership benefit. All rights reserved. No portion of this journal may be reproduced, by any process or technique, without the express written consent of the publisher.

Advertising in Maryland Medicine does not imply approval or endorsement by MedChi unless expressly stated.

DISCLAIMER: Some articles may contain information regarding general principles of law. They are not intended as legal advice and cannot be substituted for such. For advice regarding a specific legal situation, consult an attorney licensed in the applicable jurisdiction and with appropriate training and/or experience in the legal area in question.

Introduction

Stephen J. Rockower, MD

Be afraid. Be very, very afraid. This issue of *Maryland Medicine* is designed to scare you. There are many bad people in the world just waiting to get at your data. Some of them are overseas, but as we have learned in recent weeks, a few of them work right here at Fort Meade, Maryland. There are many reasons for wanting to examine your data, from cyber espionage to identity theft to counterterrorism. While no system is 100 percent safe, we must do what we can to protect ourselves from prying eyes.

This issue of *Maryland Medicine* will examine cybersecurity on a global and personal scale. We will try to give some tips and pointers on how to protect yourself, and what to do after a breach. Other recent reports have delved into the possibility of breaches in the security of electronic medical devices. Homeland security notwithstanding, the thought of pacemakers or other devices subject to hackers is truly frightening.

We start, however, with a review of the recent legislative session in Annapolis. Some might say that no one is safe when the legislature is in session, but the House of Medicine did relatively well during this past session. We were able to successfully make inroads on scope of practice issues by non-physicians, and worked diligently on public health issues such as the recent sterile compounding issue. A major update to the Board of Physicians legislation was carried out with many safeguards put into place.

In this issue there are a number of articles on various aspects of cybersecurity. We present an overview of some of the major issues of cybersecurity in the government and industrial world. We explore the use of various forms of Trojan Horses, used by the Chinese and other hackers, to get into computer systems that might have useful information. The recent news has put security and privacy on the front pages of all our newspapers, and the public dialogue of the role of the government in protecting us without violating our freedoms has become front and center. These issues need discussion in an open and thoughtful fashion, without wild rhetoric from either side.

We present a number of articles specifically designed for your medical practice. Jonathan Krasner of Business Engineering, Inc.(BEI), an IT support firm, tells us how to protect our medical systems from outsiders. Dr. Haas of DocBooks, reminds us of the common HIPAA violations that can get physicians into trouble. MedChi Insurance Agency's Ron Kendall, reminds us of the dangers of privacy breaches, and the value of insurance products when breaches occur. Additionally, Dr. Peruvemba gives us a look into the future with an overview of voice-authentication that provides security to health files.

The Department of Health and Mental Hygiene's Molly Marra and Maureen Regan, give us an outline of the increases in Maryland Medicaid payments for the primary care services that began January 1, 2013. This program, passed with the strong support of the MedChi legislative team, provides extra payments for the Evaluation and Management (E&M) services when rendered not only by "primary care" providers but for all providers. We may be the only state in the country with such a program.

We also have Dr. Barton Gershen's "Word Rounds" column. As any reader of these pages knows, these excellent articles are possibly the most erudite and well-read portion of the journal. I know his articles are always the first place I turn when I receive a new issue of *Maryland Medicine*. He is trying to retire from our editorial board, but we won't let him. His wise words and gentle spirit have enlivened many an editorial board meeting.

One more note of personal privilege: Our managing editor, Susan Raskin, has retired from this position to take on the more demanding role of grandmother. She has been the bedrock of our publication and has been invaluable with each and every issue as she has run down authors, edited our musings, and been a good friend. We wish her all the best in all that she does. We will miss her.

Stephen J. Rockower, MD, is a practicing orthopaedic surgeon in Rockville, Maryland, and a member of the Maryland Medicine *editorial board. He is also Treasurer and Trustee at Large of MedChi. He can be reached at DrRockower@CORdocs.com, or on Twitter at @DrBonesMD.*

President's Message ...

continued from page 4

Health Care) to provide a onetime payment of up to $15,000.00 to primary care practices that use electronic medical records. MedChi continues to work to expand this incentive to include all Maryland physicians. Contact Craig Behm, MedChi Network Services, at 800.492.1056, ext.3344 or cbehm@medchi.org to help navigate through this process.

This list of accomplishments is just a snippet of what MedChi does to serve physicians, their patients and the public's health. I am very proud of MedChi's advocacy efforts and of the physicians and staff that make it possible for us to fulfill this mission. Thank you all very much.

Before I conclude, I want to comment on disparities. I was recently asked by *The AMA News* to comment on a report that compared the health outcomes of Baltimore City and Howard County. I responded that it should come as no surprise that Howard County, the most affluent county in Maryland, measured the highest outcomes, and Baltimore City, the poorest area in Maryland, measured the lowest. Health outcomes were one of many parameters that were measured. The report demonstrated that economics is at the root of disparities, whether one is measuring unemployment, education, teen pregnancies, addiction, divorce, single parent families, premature deaths, assaults, murders or rapes. Our children have equal access to education but outcomes vary significantly. Disparities in education occur for various reasons, but the two leading causes are poverty and the home environment. As we now prepare to expand access to health care, disparities in health outcomes will not disappear. There are social and economic issues that need to be resolved before disparate outcomes significantly improve.

It is my opinion that the insurance industry has historically been an impediment to promoting health and decreasing unhealthy habits, along with industries that manufacture and market unhealthy products. It is difficult to incentivize insurance companies to invest in health when they provide insurance coverage one year at a time, after which the policyholder may switch to another insurance company. Just as quality of care is contingent upon continuity of care, health promotions and avoidance of unhealthy behavior is contingent upon continuous insurance coverage from cradle to grave, rather than on year to year contracts. Individuals, insurance companies and Maryland are all winners when we are healthy. We all need to be incentivized to accomplish this goal. Our body is the vessel that transports us through our lifetime and it behooves us to keep this vessel in the best working order. Health is the nectar that gives us the opportunity to extract the most pleasure from life.

Brian H. Avin, MD, practices neurology in Silver Spring, MD.

MedChi Accomplishments During the 2013 Maryland Legislative Session:

A Recap of Legislative Initiatives Impacting Physicians and Patients

Stephen J. Rockower, MD

The 431st Session of the Maryland General Assembly concluded at midnight on Monday, April 8th after its usual 90-day session. During this session, the General Assembly considered 2,619 legislative bills and resolutions. There were many important non-medically-related issues considered and passed on behalf of the O'Malley Administration, including gun control, repeal of the death penalty and an increase in the gasoline tax.

Whatever your feelings about the ACA, it is going to be implemented, and Maryland is preparing for it. MedChi was able to insert provisions to maintain continuity of care when a patient changes his/her physician, and our Assignment of Benefits provisions (passed in 2011) under these circumstances.

MedChi, the Maryland State Medical Society, considered over 750 of those bills. The Legislative Council led by James York, MD and Brooke Buckley, MD, met weekly with the MedChi lobbying team of Joseph (Jay) A. Schwartz, III, Pamela Kasemeyer and J. Steven Wise, to craft responses to these bills and formulate strategies for and against the issues. Many interested physicians participated in testimony before committees in both the Maryland House and Senate. Overall, this year from the standpoint of Medicine, was reasonably successful.

Health care was front and center with the *Maryland Health Progress Act of 2013* (SB/HB 228). This provided needed infrastructure for the coming of the Health Information Exchanges (HIE) under the Affordable Care Act (ACA). Whatever your feelings about the ACA, it is going to be implemented, and Maryland is preparing for it. MedChi was able to insert provisions to maintain continuity of care when a patient changes his/her physician, and our Assignment of Benefits provisions (passed in 2011) under these circumstances.

The Medicare Waiver allows Maryland (the only state in the Union) to follow its own rules concerning hospital rates. This has allowed at least a billion extra federal dollars to be received by Maryland hospitals. There is the possibility, however, that Maryland might not be able to continue the waiver because of recent problems with financial controls. One of the new provisions being discussed with the Maryland Department of Health and Mental Hygiene Secretary Joshua Sharfstein, MD, includes the prohibition of fee bundling.

Major Medical Issues

Naturopathic providers were again defeated in their bid to have all the rights and privileges to practice as physicians (MDs and DOs). MedChi offered compromises to allow naturopaths to function as allied health professionals, but the bill was withdrawn on the day of the hearing in the Senate committee.

The Step Therapy bill (SB764/HB1015) would have prevented insurance companies from requiring documentation that less expensive therapies and/or medications had failed, before approving more modern techniques, thus keeping the physicians' clinical judgment relevant to patient care. This was never voted on, but MedChi was able to persuade the legislative leadership to write a letter to the Maryland Health Care Commission requesting that they consider the issue through the regulatory process, or bring solutions back to the legislature by December, 2013.

There were two bills relating to Workers' Compensation and Fee Schedules that apply to medication dispensing. The bills would have drastically restricted physicians from prescribing and dispensing medications. Both bills were defeated, but will likely return during the 2014 legislative session.

The Board of Physicians (BOP) was up for re-authorization under a "Sunset Review." This had been delayed to allow Jay Perman, MD, President of the University of Maryland, Baltimore, to prepare a review.

As finally constituted from numerous bills, HB1076/SB672, provides the following:

- Increasing the Board of Physicians (BOP) from 21 to 22 members. This will allow two 11-member panels to assist with disciplinary hearings in order to speed up the disposition of cases. The majority of those on each panel will be physicians, thanks to MedChi's efforts
- Maintaining one osteopathic physician on the BOP
- Maintaining two peer reviewers for each case, despite Dr. Perman's recommendations for a reduction
- Prohibiting the BOP from administering physician rehabilitation programs and requiring a non-profit organization (such as the Center for a Healthy Maryland) to take the lead
- Allowing physicians to earn CME credits for pro-bono volunteer work in the state.

Another bill, HB1296/SB981, changed the way the BOP issues summary suspensions. Specific issues can be addressed when appropriate, rather than by insisting that the physician stop practicing altogether. In addition, there is now a more streamlined process for the adjudication of physician cases after the issuance of a Final Order.

HB1313 allows a 60-day grace period for the renewal of licenses without a penalty. The process was amended to allow either mail OR email notices (not ONLY email notices) for the renewal process.

In addition, license fees were proposed to be raised for physicians, in order to help close the state's budgetary shortfall. The state already diverts a significant portion of the physicians' licensing fees, and more are on the way. MedChi convinced the chairs of the appropriate Health and Human Resources committees to write to Secretary Sharfstein on MedChi's behalf to reconsider this. While this has not yet been finalized, it looks promising. Further meetings among the stakeholders are forthcoming.

Other issues addressed in the session included the following:

Public Health

The sterile compounding issue was high on everyone's list after the Massachusetts scandal when a compounding pharmacy was shut down after an outbreak of meningitis. Dr. Sharfstein provided leadership for SB896/HB986 to further regulate and license compounding pharmacies that ship medications into Maryland. Protections were put into place, as requested by the ophthalmologists, to allow them to "stockpile" certain drugs in advance of an unknown emergency.

Driving while using a cell phone has now become a "primary" offense, so you can be stopped by a police officer if you are observed talking or texting (SB339/HB753). Previously, you had to be stopped for another reason, as this was a "secondary" offense.

MedChi has been instrumental in promoting the safe use of "medi-spas" in conjunction with cosmetic surgery. This relates to the death in 2012 of a patient who had a procedure in an unregulated environment. HB1009, as passed, provides more regulatory power by Secretary Sharfstein to disallow certain procedures out of "public safety concerns." More work will be done to further clarify this concept.

MedChi has also been concerned with electrical reliability in medical facilities and physicians' offices. HB1159 only addressed issues related to patient and facility needs when there is a power outage, but it provides the groundwork for us to continue the conversation about providing safeguards for offices.

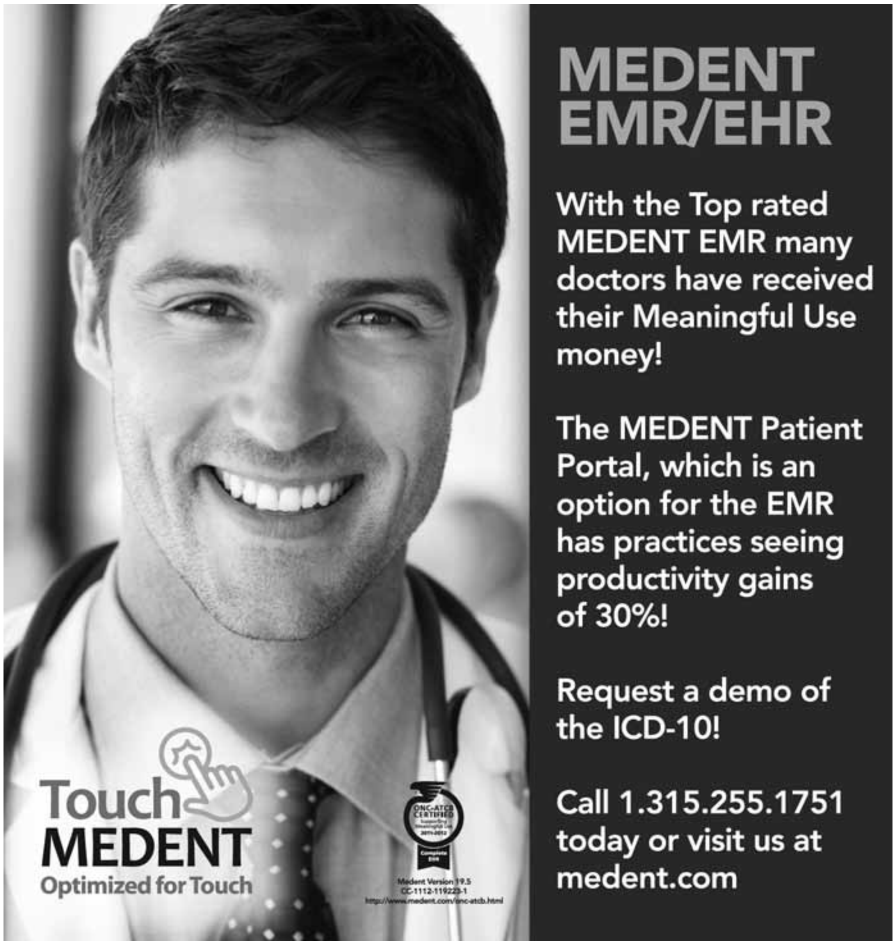
HB1270 would have outlawed the sale of tobacco in all health care facilities, including pharmacies. This did not pass but it sets the stage for next year as pharmacies try to increase the perception that they are full service health care facilities.

Malpractice

There was not much legislation related to malpractice that occurred during the session. Four bills never made it out of committee, although they would have been helpful in strengthening the "Apology Law," delaying payouts over time, and decreasing interest rates. Also omitted were nurse practitioners being included under the "cap" for non-economic damages.

The 2013 Maryland Legislative Session provided no "ground-breaking" medical issues, but served to further promote many of our concerns moving into the years ahead. Many of these issues continue to return year after year (naturopaths, cosmetic surgery, midwives, etc.), and our legislative team is working continuously during and between sessions to promote our interests. All members of MedChi are encouraged to be involved and participate in these efforts to promote health issues in Maryland.

Stephen J. Rockower, MD, is a practicing orthopaedic surgeon in Rockville, Maryland, and a member of the Maryland Medicine *editorial board. He is also Treasurer and Trustee at Large of MedChi. He can be reached at DrRockower@CORdocs.com, or on Twitter at @DrBonesMD.*



Don’t Go Near the Watering Hole: Protect Yourself from Cyber Attacks

Stephen J. Rockower, MD

“Just because you’re paranoid doesn’t mean they aren’t really out to get you.” So goes a popular meme that jokingly deals with many of the insecurities of our lives. Computers and the Internet have made all of us vulnerable to nefarious people trying to steal our identities, our money, and our secrets.

Any computer you own or type into is a potential security leak. If you are connected to the Internet – somebody, somewhere, can find you and look at your personal data. How can we protect ourselves? Around the globe governments, businesses, and individuals are all asking that question.

A quick perusal of any recent newspaper will reveal that, on any given day, dozens of companies have their computer systems breached, hacked or otherwise compromised. A recent report in April, 2013, claimed that much of the industrial espionage originates from Russia, Africa and China. These allegedly government-approved hackers try to break into any and all computer systems, whether they represent industry, government or other computer industries. Google®, The *New York Times*, Coca-Cola®, The White House, and the Department of Defense are a few of the systems that have been compromised at one time or another.

The Chinese connection, known as Unit 61398, is based in Shanghai and is thought to be part of a governmental operation to pry into the secrets of American companies and industries. The *New York Times* reported that their own systems had been breached. These attacks begin with what is known as a “watering-hole” attack, by compromising sites that are known to be frequented by people who use the information from that site. The attackers implant malicious code (called a RAT or “Remote Access Trojan”) on the site, which subsequently is downloaded to the intended target’s computer. It is called a “watering-hole” attack because lions will be at the watering hole, waiting for prey to come to them.

Once the hacker puts his code on the target’s computer, passwords and files can be passed back, usually through a variety of networks, to the perpetrator in China. The Mandiant Corporation, a cybersecurity firm in Alexandria, Virginia, traced the multiple Internet Protocol (IP) addresses of the ultimate destinations back to the building in Shanghai that houses Unit 61398. They have identified at least three people or “personas” that have been at the center of these attacks. Their code names, “UglyGorilla,” “DOTA,” and “SuperHard,” date back to 2004. These individuals have also been involved in phishing and other social engineering attacks.

continued on page 13

Security Dictionary

Phishing is an email from “Security” requesting verification of your account by re-entering names and passwords.

Spear Phishing is an email targeted at a particular group asking for “Update From Thursday’s Meeting” with an infected spreadsheet attached to it.

Whaling targets those emails at the highest levels of an organization.

Diversion links to an incorrect or similar web address to implant the malicious code.

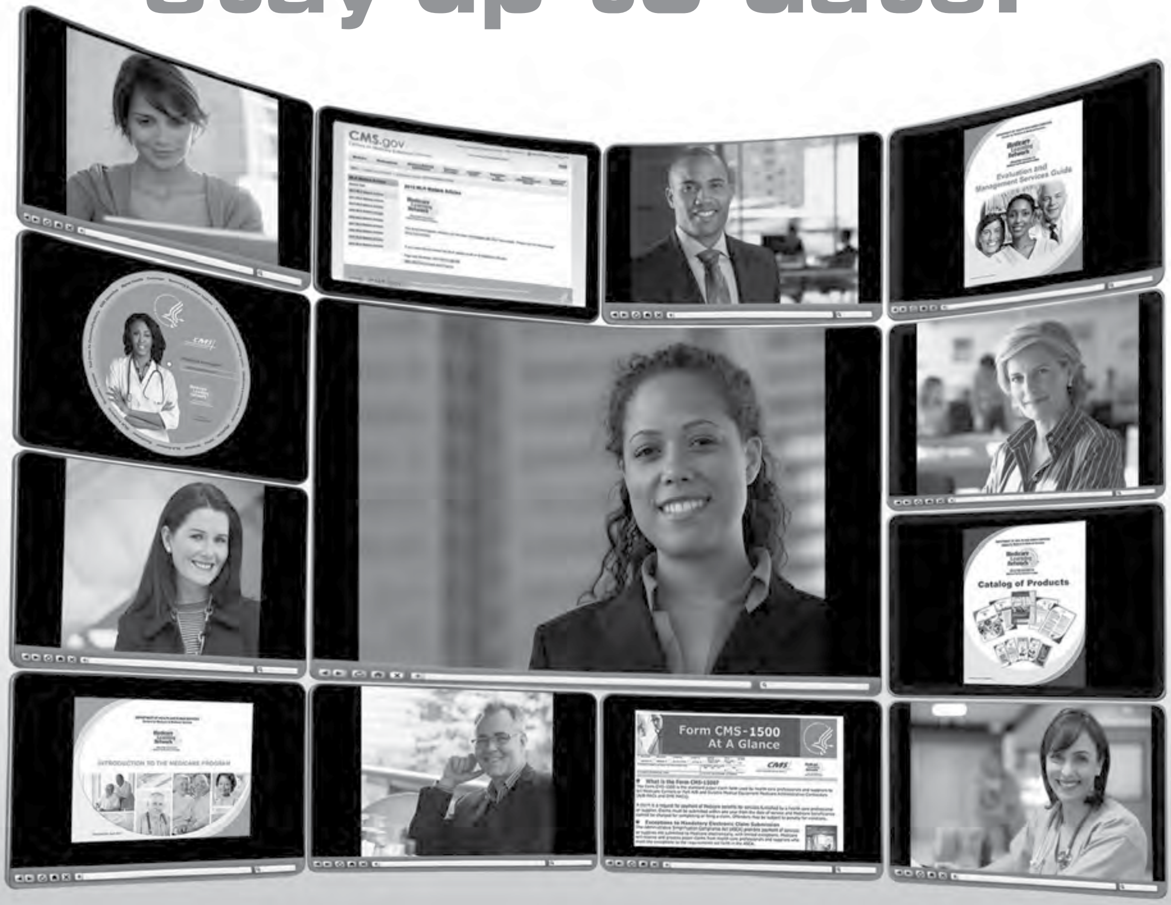
Baiting leaves an infected CD or thumb drive in the building or workplace of the target so that someone will put it in a computer and infect the network. The result is a Trojan Horse.

Pre-texting is a frantic call or email “from a grandchild” or close friend saying they’ve been arrested while on a trip and need money to get home or for “bail.”

Medicare Learning Network®

Official CMS Information for
Medicare Fee-For-Service Providers

We make it easy to stay up-to-date.


CMS.gov
Evaluation and Management Services Guide
Catalog of Products
Introduction to the Medicare Program
Form CMS-1500 At A Glance

http://go.cms.gov/MLNGenInfo_MD

As you know, every business day can bring an avalanche of information about new policies, regulations and procedures. The Medicare Learning Network® MLN is your source for official CMS information about the Medicare Program.

DEPARTMENT OF HEALTH & HUMAN SERVICES · USA

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Medicare Learning Network®
Official CMS Information for
Medicare Fee-For-Service Providers

Don't Go Near the Watering Hole ...

continued from page 11

What are the Chinese and other hackers looking for? Anything and everything. They are often searching for dissidents within their own country and for any contacts they might have with western media. They are also looking for industrial secrets such as plans for F-35 fighters, electrical plants and other infrastructure projects, and conversations between politicians. Many of the hackers are looking for credit card numbers, social security numbers and other information useful for identity theft.

Many of us have received an email that begins, "Dear Kind Sir, I am Alfred Ngobe, Solicitor for the late Prince Mbawa who died with no heirs and $20 million in a Swiss account. Could you please send your bank information so that we can wire this money into it for our mutual benefit?" The text is fraught with sob stories to encourage the mark to open their hearts and their wallets. Usually, there are atrocious spelling errors and extremely poor syntax. It is amazing that anyone actually falls for these schemes, but millions of dollars are lost each year. These are often called "419" scams, named after the section of the Nigerian penal code that outlines the offense. These kinds of scams are not new. Variations have been around since the 1920s as the "Spanish Prisoner" scam, and even earlier. After the French Revolution at the end of the 18th century, perpetrators claiming to be in the domestic service of imprisoned bourgeois noblemen, were sending letters requesting financial assistance to intended targets.

Other types of RATs that get implanted in computers and related equipment include, "distributed denial of service" (DDOS) software. This RAT connects circuits around the world that can then simultaneously access a particular website, such as whitehouse.gov or Apple.com. The millions of computer requests overwhelm the attacked system, and the website crashes. It can take hours or days for the attacked system to get up and running again. You may never know that your computer is part of this robot network, or "bot-net," that is helping to take down the Department of Defense.

Another type of infection is "scareware" or "ransomware". These programs will pop up and inform you that you are infected, and that a credit card number is required to buy the removal tool. Or, they will scare you even more by threatening to wipe your hard drive and delete all your files. Others will turn on the cameras and microphones in your computer to listen to conversations and take pictures of you and those around the computer.

What should you do to protect yourself and your company? First and foremost, have proper antivirus software installed. These are available from Symantec (Norton), MacAfee, Kepersky, AVG, Avast and others. Most are on a subscription basis, though some are free. Just having the software is not enough, however. It MUST be regularly updated, as new scams are appearing every week. In addition to the antivirus, your browser needs to be up to date. Internet Explorer, Firefox, Chrome, Opera and others regularly put out security updates. These systems download the updates in the background, but often your machine needs to be rebooted for the updates to take effect. Other security programs include Malwarebytes, Spybot Search and Destroy, Windows Defender and WinPatrol.

Once your browser is "relatively" secure, you need to practice safe computing.

Safe Computing

- DO NOT click on a link from an unknown sender. Even when the sender is known to you, be sure the message is not unusual for them to send. Spammers can hijack your friend's address to send you a malicious link that might say, "Hi, I saw this and think you'd like it!"
- If the link is suspect, you can hover your mouse over it <without clicking> to see the address it is actually pointing toward (often in the bottom left corner of your screen). If that address looks wrong (with a .ru, .cz, or other foreign code), delete the email.
- Use strong passwords. The most commonly used password is "password," followed by "123456," "abc123," and "qwerty." These are easily guessed by even the dumbest crooks. Use a combination of upper and lower case letters, combined with number5 and punctuation. Substitute numbers or symbols for letters: v3gg!eWr4p or 5ecUr1ty. These are examples that are understandable, easy to remember and reasonably strong.
- Strong passwords can be generated for you by password programs like KeePass, RoboForm, LastPass, 1Password or SafeID. With one "master" password, a cloud-based program will maintain very secure passwords for different sites and fill them in for you. Obviously you shouldn't use this for an unsecured computer.
- Online banking is fine from home (assuming you have followed the above rules), but NEVER access a secure site from a free wifi location such as Starbucks. These open connections allow lurkers at the next table to monitor the traffic over that network and capture your keystrokes and passwords.
- Backup, Backup, Backup. Your data is your most valuable asset. Have it offsite on an external drive or in the cloud with Carbonite, Norton, Google Drive, Backblaze, to name a few. This can be done automatically. You never know when disaster can strike, whether you are in New Orleans, Seaside, NJ, or Moore, Oklahoma. Computers can be replaced, but data cannot.

Remember that no system is 100 percent secure. Many large companies and organizations are abandoning the "citadel" model of security – keep all intruders out – in favor of the "prison" model – let them in but make them miserable once they are there. Internal security includes encrypted data and often non-password-enabled verification that include fingerprints, iris scans, or security questions. The best security questions cannot be easily guessed or researched by someone looking for your data. Your mother's maiden name is probably in somebody's genealogy website or on your online marriage license. Google has instituted a two-step verification process that will send a text to your cell phone that has to be input before you are allowed to sign in. This is obviously very secure unless you lose your cell phone. The hassle factor runs high.

Security is everyone's business. Nothing is absolutely secure, but we all need to take steps to ensure that what we are doing is reasonable and safe in our modern world.

Stephen J. Rockower, MD, is a practicing orthopaedic surgeon in Rockville, Maryland, and a member of the Maryland Medicine editorial board. He is also Treasurer and Trustee at Large of MedChi. He can be reached at DrRockower@CORdocs.com, or on Twitter at @DrBonesMD.

CELEBRATING **45** YEARS

Improving *the Practice of Medical Billing and Collecting*

Since 1968, PMI has specialized in advanced practices for medical billing, collections, coding and follow-up services. We deliver **sound revenue-building consulting services** to physicians and medical practices through **innovative technology and unmatched local expertise.**

PMI
Medical billing is **our business**

Professional Management, Inc.
9900 Franklin Square Drive, Suite B
Baltimore, MD 21236
Toll-free: 855.764.2455
www.pmi-web.com

Healthy loans for a healthy business.

- INCREDIBLY LOW RATES
- NO LENDER FEES
- NO PREPAYMENT PENALTIES
- FAST, PERSONAL SERVICE

Let us help you build a better business.
Visit **nihfcu.org/businessloans**
or call **877.398.4892**.

nih Federal Credit Union
The nation's largest credit union serving the biomedical industry.

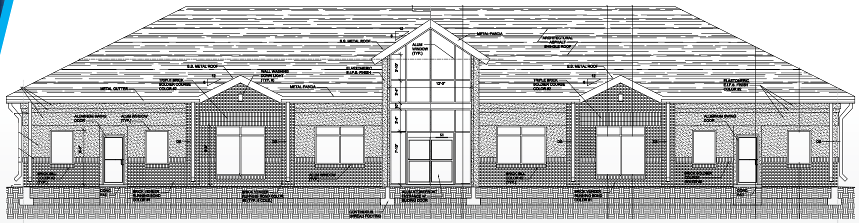
NCUA Federally insured by NCUA.

OFFICE SPACE

IDEALLY SUITED:

- Medical practice
- Ambulatory surgery center
- Healthcare services
- Urgent care center

LOOKING TO EXPAND?



123 Singerly Avenue, Elkton, MD 21921

Over 40 physicians within one block area
Located directly across from Union Hospital
Available area from 1400-4000 Sq Ft

Phone number: (410) 635-0399 / lease@123singerlyavenue.com

Cybersecurity and Your Practice: What You Need to Know

Jonathan Krasner

Hardly a day goes by without some type of major cybersecurity issue in the news. Several high profile organizations have recently suffered security breaches including the *New York Times*, Coca Cola, The Associated Press, the Department of Energy and Booz Allen Hamilton. And not all companies report their security breaches to the government or announce them to the press, so there are likely many more that we just haven't heard about.

Health care practitioners are certainly not immune to this kind of hacking. The Health Insurance Portability and Accountability Act (HIPAA) rules require the disclosure of events when unsecured Protected Health Information (PHI) is potentially breached. The list of reported security breaches on the Department of Health and Human Services (HHS) website (hhs.gov), currently lists 607 separate reported incidents. As more and more PHI moves from paper to electronic records, the potential for security breaches will only rise.

Proper cybersecurity practices are necessary for any business as cyber rules and regulations are imposed on many industries. All publicly-held companies must comply with the Information Technology (IT) security requirements of the Sarbanes-Oxley Act passed in 2002. Any organization that does business with the government has to comply with the Federal Information Security Management Act (FISMA).

In the health care industry we have HIPAA, which was initially enacted in 1996 and has been amended several times, most recently in 2013. When HIPAA was enacted, most, if not all practices used paper medical records. HIPAA compliance for paper records is easy to achieve and does not require significant effort on the part of a practice. Such is not the case with electronic records.

Before discussing specific common cybersecurity practices, it is important to understand that the HIPAA Security Rule requires that each practice conduct a security risk analysis of its computer network. HHS felt so strongly about this that the risk analysis, in addition to being a HIPAA requirement, is a core measure by the Centers for Medicare & Medicaid Services (CMS) for both Meaningful Use Stage 1 and Stage 2.

What is a risk analysis? A risk analysis is the process by which an organization undertakes to identify potential threats to and vulnerabilities of their information systems, and then assesses the associated risks. Once these risks are identified, the practice can then put a plan in place to eliminate or remediate them. Because every practice has a different network and software system, there is no "one-size-fits-all" template for a risk analysis. In fact, HHS guidance specifically states that, "[t]here is no single method or 'best practice' that guarantees compliance with the Security Rule." However, most outpatient medical practices are sufficiently similar, so there are some basic policies and procedures that should be considered by all.

See Basic Cybersecurity Checklist on next page

Basic Cybersecurity Checklist

Policies and Procedures

- □ All security-related policies and procedures should be carefully considered and documented in writing. Your IT support vendor should be able to help you with this effort. (Side note: Your IT support vendor is considered a Business Associate by HIPAA, and with the release of the most recent Final Rule in January 2013, should be HIPAA compliant themselves. You should verify your IT support vendor's HIPAA compliance.)
- □ All employees should go through HIPAA security training, including how to spot suspicious emails and websites. Many security breaches occur when employees unwittingly click on malicious links that lead to computer viruses and other malware.
- □ Policies and procedures should be reviewed and revised appropriately once per year.

Software

- □ Every employee should be assigned software access rights based on their role in the practice.
- □ Every employee should have a unique ID/password. Implement strong password requirements of at least eight alphanumeric characters. Require passwords to be changed at least every 180 days.
- □ EHR applications and any other applications that contain PHI should "lock" after 10-15 minutes of inactivity.
- □ In high traffic areas (such as hallways), install privacy screens on monitors.
- □ Use business class anti-malware software that can be centrally monitored to assure that it is kept up-to-date.
- □ Make sure that operating systems (e.g., Windows, Linux, OSX, etc. for both servers and desktops/laptops) are kept current. All OS vendors, Apple included, issue patches every month that can be downloaded for free. Most patches involve improving security – either plugging an existing hole or protecting against a new threat.

Email

- □ Never send PHI over regular email. Regular email is not encrypted. If you don't know if your email is encrypted, assume it is not. (Note: Encryption is the process of encoding information in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can.)
- □ Patients may send you emails with PHI, but do not send a response with any PHI.
- □ Use a secure Patient Portal to communicate electronically with patients.
- □ Consider using DIRECT email messaging to communicate with other providers. DIRECT is a new secure, encrypted email system just for healthcare professionals. In the state of Maryland, it is offered by CRISP, the Health Information Exchange. You will most probably need to use DIRECT messaging to comply with Meaningful Use Stage 2.

Hardware

- □ Encrypt all laptops and tablets with FISMA-compliant encryption (FIPS 140-2 is the relevant requirement). Laptops and tablets are highly susceptible to loss and theft. If you lose one of these devices you are not required to report it to HHS if the device was encrypted and you have documentation to support that assertion.
- □ Consider encrypting desktops, servers and copy machines. Even though these devices are much less susceptible to loss or theft, it is possible that they can disappear.
- □ Make sure that all hard drives have no PHI when disposing of a device. A common practice is to get a certificate of destruction from an electronic recycling vendor.
- □ Secure your wireless network. This certainly means a strong password, proper encryption and even non-broadcast of the SSID. A wireless network for your patients should be separate and outside your primary IT infrastructure.
- □ Make sure your network is protected with a business class firewall that is properly configured. A Linksys router that you buy at Best Buy is NOT business class. Business class is WatchGuard, Cisco, Sonicwall, etc.
- □ Prohibit the use of thumb drives for storing PHI. They can easily get misplaced.

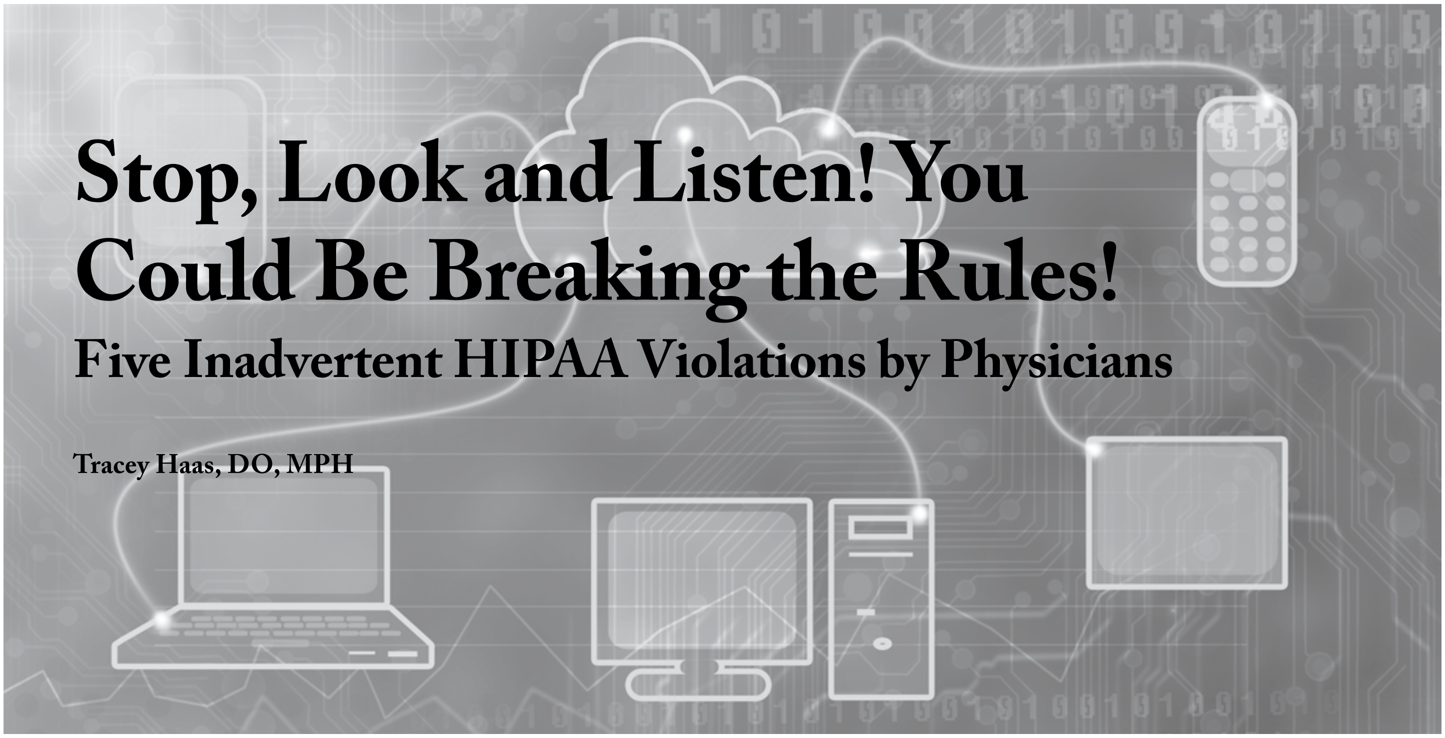
It should also be noted that HIPAA compliance goes beyond the above security issues and should address other concerns such as privacy and backup/disaster recovery planning. This basic cyber checklist is a good start. Remember, every practice's network is different and needs to adopt appropriate individualized policies. The good news is that there are many resources available to help you with this. After proper policies and procedures have been implemented, maintaining compliance should not be burdensome to you or your staff.

Jonathan Krasner is a health care IT consultant for BEI, Business Engineering, Inc., a Reston, Virginia-based provider of IT support services to practices of all sizes throughout the Washington, D.C. metropolitan area. He can be reached at Jonathon.krasner@beinetworks.com.

Stop, Look and Listen! You Could Be Breaking the Rules!

Five Inadvertent HIPAA Violations by Physicians

Tracey Haas, DO, MPH



Physicians do not plan ahead to violate the Health Information Portability and Accountability Act (HIPAA), but in this digital age, they may be doing so because they did not plan ahead. The recent final rule of the Health Information Technology for Economic and Clinical Health (HITECH) Act indicates that even if the physician is unaware of the violation, they may be fined a civil penalty of $100 - $50,000 per violation. It is time for even the most resistant physicians to pay attention to how they handle Protected Health Information (PHI).

Below are five common ways that physicians are breaking HIPAA/HITECH privacy and security rules, and may not even know it.

Should You Text Protected Health Information (PHI) to Members of the Care Team?

Here is a simple scenario: You have just left your office and your nurse texts you to say that Mrs. Smith is having a reaction to the medication you have just prescribed. She has given you the patient's name and contact information so that you may contact her. Even if you know that contacting her is not legal, you feel justified in doing so because this could be a serious medical issue. Perhaps you even believe that deleting it right away will protect you – and Mrs. Smith. In reality, this information has just passed from your nurse's phone, through her phone carrier, to your phone carrier, and then to you – four vulnerable points where this unencrypted message could either be intercepted or breached. In a secure messaging application (app), this type of message is encrypted as it passes through all four points of contact, and the recipients are verified.

Should You Take a Photo of a Patient on Your Mobile Phone?

If patient photos are viewed by those for whom they are not intended, you may be in violation of HIPAA. There are apps that allow photos to be taken within the secure messaging app itself – never stored on your phone or within your phone's photo album. You should always use this type of feature when taking any photo of a patient or patient information.

Should You Receive Text Messages from Your Answering Service?

Many physicians believe that if they receive a message from a third party, like an answering service, they are not responsible for a HIPAA violation. This is simply not true. Many services do send a patient's name, telephone number and chief complaint via a short message service (SMS) text. They may verify that it is encrypted on their end, but if it pops onto your screen, it is certainly not secure on your end – and this is where your responsibility lies. Talk with your answering service to see how they are protecting you at both ends of the communication.

Should You Allow Your Child to Borrow Your Phone?

Many parents allow their children to play with their phones. If your phone has an app that can access PHI, and you share that phone with your children, then you may be guilty of a HIPAA breach. The simple fix is to utilize the pin-lock feature on your messaging app – and for extra protection, always password-protect your phone!

What Happens If You Do Not Report a Lost or Stolen Device that Contains PHI?

Losing your smartphone or tablet is a problem for many reasons. Did you know that if you have patient information on that device, you could be held responsible for a HIPAA breach if you do not report the loss immediately? The ability to remotely disable an app that contains or handles PHI is an absolute must for

Steps to Protect Your Practice Against Cyber Attacks

Local Versus International Needs

Ruben Mbon

The U.S. Department of Health and Human Services (HHS) published the final HIPAA Security Rule in February, 2013. In the wake of this, many physicians and other health care providers are struggling to protect their patients' electronic health information against cyber criminals and to understand and comply with the new requirements in this rule. Daily high-profile cyber attacks and increased enforcement of the law by the HHS Office of Civil Rights, are only increasing the pressure on physicians and other health practitioners to become compliant as soon as possible.

Here are some tips to follow to reduce your practice's exposure to cyber attacks and improve compliance with the law.

1. Conduct a risk analysis/assessment. A risk assessment is to cybersecurity what a physical exam is to general medicine. It is the first requirement of the HIPAA Security Rule and is the foundation of a security plan. It allows you to identify your organization's assets, threats and vulnerabilities in order to determine the risks, and then consider solutions.

2. Implement some simple security controls. These tips, when implemented, will enable your practice to reduce its exposure to cyber attacks, improve compliance with the HIPAA Security Rule, and prove due diligence.

Internal controls that will improve compliance with the HIPAA Security Rule

- **Requiring** complex passwords that are regularly changed and kept private
- **Developing access controls** that create unique user-accounts for each staff member with access to your network
- **Encrypting** patients' information as well as other sensitive data in order to guarantee confidentiality
- **Limiting Internet access** to reduce your practice's exposure to all types of Internet-related attacks
- **Using anti-virus software** to protect your systems against malicious code attacks
- **Installing firewalls** to protect your network against unauthorized access
- **Writing policies and procedures** for all of your security measures for staff to access and agree to
- **Encouraging a security awareness culture** within your practice to reduce risks to staff
- **Implementing the required security controls.**

These tips, when implemented, enable your practice to reduce its exposure to cyber attacks, improve compliance with the HIPAA Security Rule and prove due diligence.

Ruben Mbon is a cybersecurity engineer, founder and CEO of Unified Cyber Solutions, LLC, a cyber-security and compliance consulting company located in Maryland. He holds a BS in cybersecurity from the University of Maryland and holds many industry certifications. He can be reached at r.mbon@unifiedcybersolutions.com or 1-855-882-9237, ext. 800.

Stop, Look and Listen ...

continued from page 17

technology that handles communications in the medical space. Be sure to ask for this feature from any company claiming to help you be HIPAA-compliant in the mobile world.

Remember: Being HIPAA compliant is an active process. A device can claim to be HIPAA-secure, but it is a person who must ensure compliance.

Reference:

1. The Office of the National Coordinator's official site for mobile devices and HIPAA is http://www.healthit.gov

Tracey Haas, DO, MPH, is Co-founder and Chief Medical Officer of DocbookMD. She is a board-certified family physician and has practices in Austin, Texas. DocbookMD partners with medical societies around the country to bring their physician members a free, HIPAA-secure messaging app, that uniquely provides extra security to avoid each of these potential pitfalls. For more information contact docbookmd.com or 1.888.930.2048.

Privacy/ Data Breach Coverage: Protect Your Practice

Ron Kendall

How prepared is your medical practice for a data security breach? Increasing reports are surfacing every day about medical practices that have experienced some form of data breach, from online hackers to the carelessness of staff who may have inadvertently disposed of medical records in error. Such an error was reported last month regarding a practice in Laurel, Maryland, where hundreds of files were accidently discarded in a dumpster during an office move. In another recent report from Charlotte, North Carolina, an anesthesiology practice experienced a cyber attack due to a security flaw in the practice's website, and over 9,000 patient records were compromised.

The exposure vulnerability to cyber attacks and viruses due to careless handling of patient files on mobile technology is skyrocketing. Protected Identifiable Information (PII) that includes patient medical information, can be lost or stolen which may lead to crimes such as identity theft. HIPAA regulations require medical offices to handle Protected Health Information (PHI) with a stronger "duty of care" than other businesses. Newly established data breach notification laws require notification of individuals whose PHI has been lost or stolen. These laws have created standards of care under which a lawsuit can be based. In addition to fines, penalties and response costs, physicians may face civil lawsuits for tort damages arising from a breach.

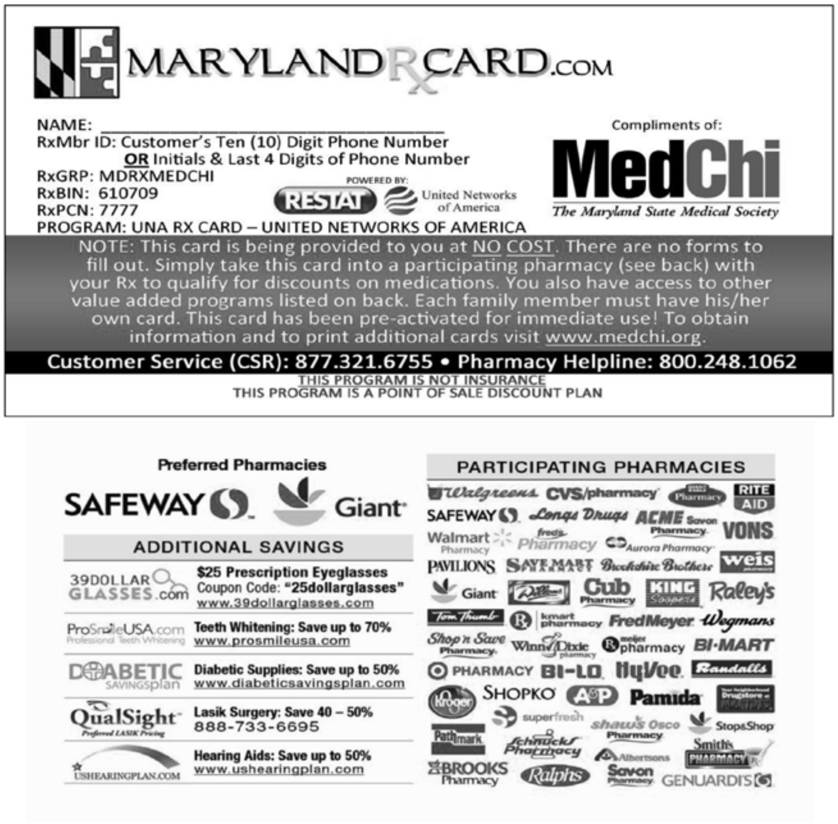
Privacy/Data Breach coverage is one of the best ways to protect yourself. There are several methods by which it can be obtained: as a stand-alone policy offering the maximum in protection; by an endorsement to your business office policy through several property and casualty carriers that offer minimal coverage and limits; or as part of MedGuard, offered through Professional Advocates/Medical Mutual Liability Insurance Society of Maryland, in conjunction with Administrative Defense with shared limits.

For more information and a consultative review of your practice's possible exposure to a Privacy/Data Breach, please contact Ron Kendall, Business Development Manager, at the MedChi Insurance Agency. He can be reached at 410.539.6642, ext. 4431 or at RKendall@medchiagency.com.

Components of Privacy/Data Breach Coverage

- Provides the cost of Third Party notification. The average cost for a patient's record breach can run $300-$400 per patient.
- Provides costs to keep the practice compliant. These expenses will include notification costs, credit monitoring and legal services. In addition, it provides public relations and good faith advertising plus defense and liability expense coverage.
- Provides coverage for civil fines and penalties related to HIPAA violations.
- Provides coverage for breach as a result of stolen mobile technology and paper files.
- Provides coverage for information breached from use of printers, scanners and fax machines.

Success by MedChi has partnered with Maryland Rx Card to offer you and your family access to a **FREE** DISCOUNT HEALTH SAVINGS CARD. Simply cut out the free card below and receive savings of up to 75 percent (savings average around 30 percent). All prescriptions processed through the program are completely confidential. This program includes discounts on Prescriptions, Eyeglasses, Hearing, Nutritional Supplements, Diabetic Supplies, and more. This card is pre-activated and can be used immediately! For more information contact Erin Krell: 800-492-1056 ext. 3304



MARYLANDRxCARD.COM

NAME: ______________________________
RxMbr ID: Customer's Ten (10) Digit Phone Number
OR Initials & Last 4 Digits of Phone Number
RxGRP: MDRXMEDCHI
RxBIN: 610709
RxPCN: 7777
PROGRAM: UNA RX CARD – UNITED NETWORKS OF AMERICA

POWERED BY: RESTAT United Networks of America

Compliments of: MedChi *The Maryland State Medical Society*

NOTE: This card is being provided to you at NO COST. There are no forms to fill out. Simply take this card into a participating pharmacy (see back) with your Rx to qualify for discounts on medications. You also have access to other value added programs listed on back. Each family member must have his/her own card. This card has been pre-activated for immediate use! To obtain information and to print additional cards visit www.medchi.org.

Customer Service (CSR): 877.321.6755 • Pharmacy Helpline: 800.248.1062

THIS PROGRAM IS NOT INSURANCE
THIS PROGRAM IS A POINT OF SALE DISCOUNT PLAN

Preferred Pharmacies

SAFEWAY Giant

ADDITIONAL SAVINGS

39DOLLARGLASSES.com	**$25 Prescription Eyeglasses** Coupon Code: **"25dollarglasses"** www.39dollarglasses.com
ProSmileUSA.com Professional Teeth Whitening	**Teeth Whitening: Save up to 70%** www.prosmileusa.com
DIABETIC SAVINGSplan	**Diabetic Supplies: Save up to 50%** www.diabeticsavingsplan.com
QualSight Preferred LASIK Pricing	**Lasik Surgery: Save 40 – 50%** 888-733-6695
USHEARINGPLAN.COM	**Hearing Aids: Save up to 50%** www.ushearingplan.com

PARTICIPATING PHARMACIES

Our government gives you new standards.
Payers give you new requirements.
Annapolis Billing Services gives YOU the answers.

Voice Authentication - Enabling Secure and Convenient Access to your Personal Health Information

Ramani Peruvemba, MD

A primary tenet of the Affordable Care Act (ACA) is the seamless exchange of personal health information between physicians, hospitals and patients. The ACA and its Stage 2 Meaningful Use also calls for providing patients with online access to health records and secure electronic communications. Few question the benefits of increasing communication and dialogue between patient and provider – it can only lead to better health and better outcomes. Given the nature of the world today, it is likely that any communications outside of the exam room will be electronic and mobile. Of significant concern in a digital exchange of health data, is the security and privacy of such data and the supporting systems. The security of these systems may also impact physician and hospital reimbursement.

Currently, access to electronic health record security is safeguarded only by the use of a password. Such passwords can be easily lost, shared or forgotten, causing breaches in security of these systems. In fact, the shortcomings of password-based security measures are well-documented. In addition the future of medicine calls for patient access to multiple databases of health information, often necessitating multiple passwords.

The development of alternative authentication systems is currently an area of great interest, and biometrics may represent a safe and convenient approach to meet these security needs. Biometrics provide advantages over traditional password-based methods because they are not easily shared and cannot be forgotten, written down or stolen. Several biometric approaches exist, including fingerprint, facial recognition, iris recognition and voice recognition. Iris recognition has the lowest adoption because it is intrusive by its nature – most people just don't want to shoot a laser into their eye. Facial recognition is less intrusive, but only marginally so. Both fingerprint and voice-based approaches would meet user acceptance, but voice recognition may be the most practical alternative because of the following advantages:

- Voice recognition uses the most natural form of human expression – speech.
- The hands-free nature of voice authentication may be particularly useful in a critical care unit setting.
- The system can be integrated with electronic health record (EHR) systems as well as portable devices such as mobile phones and laptops.
- Such an authentication system is configurable to multiple applications and environments, and is scalable since registration can be completely automated.
- The only hardware requirement for a voice recognition system is a microphone, which is present on most if not all mobile devices and desktop computers.
- Voice recognition systems measure the unique size and shape of vocal tract features and can only respond to a particular person's voice.
- The voice recognition system will be language-independent since it is measuring vocal features rather than the specific words themselves.

In the future, as protected patient information is shared between hospitals, physicians, health information exchanges and patients, voice authentication systems appear to represent the best option for enhancement of security in a convenient and usable format.

Ramani Peruvemba, MD, is the Founder and Chief Medical Officer of Health Solutions Research, Inc., a nonprofit dedicated to researching solutions for the healthcare space. He is also an anesthesiologist practicing in Rockville, MD.

Maryland Medical Assistance Increases Payment for Primary Care Service

Molly Marra and Maureen Regan

Starting January 1, 2013, Maryland began paying most Medicaid providers a higher rate for certain primary care services, making Maryland Medicaid rates competitive with private insurance. Under the Affordable Care Act (ACA), states must pay specific primary care providers higher rates for designated primary care services provided to Medicaid recipients. The intent of these nationwide rate increases is to encourage greater primary care physician participation in Medicaid programs as coverage expands to more Americans in 2014.

Maryland Medicaid increased rates for certain Evaluation and Management (E&M) services and vaccine administration under the Vaccines for Children (VFC) Program by roughly 20-25 percent, to 100 percent of the Maryland Medicare rates, for services provided between January 1, 2013, and December 31, 2014.

While recently-released federal guidelines limited the eligible providers for increased rates, Maryland expanded provider eligibility for increased rates to most Medicaid providers. The Final Rule, released by the Centers for Medicaid and Medicare Services (CMS) in November, 2012, limited eligible physicians to general internists, pediatricians, and family practitioners. Additionally, these physicians must either be board-certified or be able to prove that at least 60 percent of the services they bill are for the eligible E&M and VFC administration services. Maryland, however, expanded eligibility for increased rates to most providers, including physician specialists, OB/GYNs, nurse practitioners and safety net providers such as local health departments and school-based health centers.

Another area where Maryland policy differs from the national norm is the unexpected Final Rule requirement that physicians self-attest to their eligible specialty before receiving the increased rates. Maryland was able to start paying the increased rates to providers much earlier than other states because attestation is not a requirement. Maryland is the only state taking this approach.

The CMS criterion for Maryland to obtain millions in available ACA funds, however, remains the same. Therefore, it is still critical for Maryland Medicaid to collect the maximum amount of CMS-eligible physician self-attestations for general internists, pediatricians, and family practitioners.

Maryland has faced an uphill battle collecting self-attestations which has spurred an aggressive campaign to get physicians onboard. Beginning in mid-March 2013, Maryland Medicaid and its outreach partners, including its eight managed care organizations (MCOs), and professional associations, began educating providers about Maryland's unique implementation of the PCP Fee Increase and the importance of self-attestation. The state has created a secure and user-friendly online attestation form to maximize self-attestations. MCOs and physician associations sent thousands of emails and letters, asking physicians to self-attest using this form to help the state obtain maximum federal funds. The state is also working in collaboration with its eight managed care organizations and various physician associations, including MedChi, to orchestrate a massive outreach effort to obtain as many attestations as possible. To date, thanks to this coordinated messaging, Maryland has collected over 3,000 attestation forms. More attestations equal more federal dollars that Maryland can spend on improving access to quality primary care.

As Maryland Medicaid's primary care service rates are now at least competitive with (if not higher than) those of private insurance plans, physicians are showing more interest in enrolling as Medicaid providers. MedChi CEO Gene Ransom, III, was recently quoted in the Baltimore Business Journal as saying that for the first time in his 17-year career at MedChi, physicians have asked how to sign up for Medicaid.

It is unknown whether the increased payment will extend beyond 2014, but for now, the effort to reach Maryland's eligible Medicaid providers is working. If you have not yet submitted an attestation for the PCP Fee Increase, you may do so at: dhmh.maryland. If you would like more information about the PCP Fee Increase in Maryland or have questions about the PCP Fee Increase, please visit: dhmh.maryland.gov.

Molly Marra is the Division Chief of Health Services Policy in the Office of Health Services with Maryland Medicaid. She may be reached at mmarra@dhmh.state.md.us or at 410-767-5949. Maureen Regan is the Publication and Communications Analyst in the Office of Health Services with Maryland Medicaid. She may be reached at Maureen.regan@maryland.gov.

Red Roses, Beautiful Eyes, and the Tropics

WORD ROUNDS

Barton J. Gershen, MD
Editor Emeritus

In the world of botany, the order of roses (*Rosales*) includes many ornamentals, among them roses, flowering cherries, mountain ash, hawthorne, and spirea. The Spirea family contains over 100 shrubs native to the northern temperate zone. An extract from one of these plants, *Spirea ulmaria* ("meadow sweet"), has an unpleasant tart flavor and was called *spiroylige saure* by researchers at the Bayer Company in Germany. (German *spiroylige*: "spirea" plus *saure*: "sour"). Bayer chemists soon learned that the principal ingredient causing that acerbic taste was **salicylic acid** (Latin *salix*: "willow" – salicylic acid had originally been obtained from the bark of willow trees). In 1899 Felix Hoffman and Herman Dreser, chemists working for the Bayer Company, developed an acetylated product of salicylic acid from coal tar (**acetylsalicylic acid**). This chemical was found to be analgesic (Greek *an*: "without" *algesis*: "sense of pain."), and much less offensive to the digestive system than the parent compound. They took the "**a**" from acetyl, the "**spir**" from *spiroylige* and they added "**in**" – calling the new compound **aspirin**. The Bayer Company began marketing this medication in 1905 and it soon became the world's largest selling over-the-counter remedy.

> When the sun reaches its lowest and highest points, it appears to **stop** moving for several days, then it turns and begins either its ascent or descent. These times are known as the winter and summer **solstice**. That term derives from Latin sol: "sun" and sistere: "to stop" – the sun literally appears to stop its vertical movement for a short while before turning and moving in the opposite direction. The word **armistice** has a similar derivation, meaning "a halt to arms or warfare." It's a very nice word. It should be used more often.

Shortly afterward, I.G. Farbin Industries – German manufacturers of weapons for two world wars – purchased the Bayer Company and established a subsidiary corporation in the United States. At the end of World War I their American business was condemned as "spoils of war" by the United States Alien Property Custodian Francis P. Garvan, and was sold to the Sterling Drug Company of New York City. The Sterling Company, founded in 1901, may be equally famous for its ownership of the D-Con company, which has manufactured and sold the rat poison **Warfarin s**ince 1947.

The story of Warfarin's discovery is interesting. **Sweet clover** is a grass cultivated and dried into hay for cattle. In 1933, farmers in Wisconsin observed that their cattle were mysteriously hemorrhaging and dying. They approached Dr. Karl Paul Link, Professor of Biochemistry at the University of Wisconsin, and requested his help. After a lengthy analysis, Dr. Link discovered that the sweet odor of clover was derived from the chemical **coumarin**, contained in its stem and leaves. (It is the cause of the sweet smell of newly-mown hay.) Morever, Dr. Link found that during rainy seasons, fungi such as the genus *Aspergillus*, grew abundantly within the hay stacks, and were capable of converting coumarin into a chemical known as **dicumerol**. He further discovered that dicumerol had significant anticoagulant properties, which explained the mysterious hemorrhagic bovine disease. Starting in 1941, physicians began using dicumerol as an anticoagulant in patients with venous thromboembolic disease, and in the 1950s they began to utilize it in patients with myocardial infarction.

Some years later, a 4-hydroxy coumarin derivative was synthesized in Link's laboratory, and found to have more predictable anticoagulant effects. They named this new drug **Warfarin**, an acronym for **W**isconsin **A**lumni **R**esearch **F**oundation plus coum**Arin**. (Warfarin depresses clotting factors II, VII, IX and X by interfering with the action of vitamin K necessary for gamma carboxylation of precursor proteins. Warfarin's trade name is **Coumadin**).

The name *Aspergillus* derives from its microscopic appearance. Some pious – but imaginative – microbiologist thought that the fungus looked like an **aspergillum** under the microscope. An aspergillum is the brush utilized by clergy to sprinkle holy water. (Aspergillum stems from the Latin *aspergere*: "to spray.")

Another anticoagulant, **heparin**, was actually misnamed – an error perpetrated by the eminent physiologist William Henry Howell, who had taught at Harvard and later became Dean of Johns Hopkins School of Medicine (1899-1911). Howell had discovered a phospholipid derived from canine liver, which acted as an anticoagulant. He believed this to be the substance which prevented conversion of prothrombin to thrombin, and he named it for its presumed site of origin. (Greek hepar: "liver.") It wasn't until 20 years later, when an acid mucopolysaccharide was isolated from beef lung by doctors A.F.Charles and D.A.Scott, that the source of heparin was correctly identified. Since then our commercial product has been derived from lung or intestinal mucosa, but the hepatic malapropism remains.

Other drugs have similarly interesting etymologies. Consider **atropine** for instance. It is an alkaloid derived from belladonna, hyoscyamus, or stramonium, and is a powerful anti-cholinergic and anti-spasmodic. Atropine may also be quite lethal in high doses, and was therefore named for one of the three mythical Greek **Fates**. The Fates were thought to spin the thread of life using either gold, silver, or woolen thread. **Clotho** places a strand (of life) onto the spindle, **Lachesis** measures its length, and **Atropos** cuts it off. (Greek atropos: from a: "not" and tropos: "to turn," therefore "not turning back." When atropine is used in large doses, death is virtually inevitable, and death is certainly one of those states from which there is no turning back.) Atropine is typically derived from the Atropa belladonna plant, whose common name is "**Deadly Nightshade**." There's a good reason for that name.

Henbane is a foul-smelling plant which is also a member of the Nightshade family. It is the source of **Hyoscyamine** and **Scopolamine**, anticholinergic relatives of atropine. (Middle English bane: "the cause of misery and death," as in "you are the bane of my existence." Chickens that inadvertently ate henbane often died from its anticholinergic effects. Dogbane has a similar origin.)

Hyoscyamine derives from Greek hyoskyamos: "pigbean" – a reference to its odor. **Scopolamine** is named for the genus of plants (Scopolia) from which it derives. Scopolia in turn originates from **Giovanni Antonio Scopoli**, an Italian naturalist (1723-1788) for whom the genus was named. **Belladonna** stems from Italian – bella: "beautiful" and donna: "woman," a reference to the fact that the drug was used to dilate pupils of desirable maidens for cosmetic effect.

The anticholinergic **Stramonium** is derived from the *Datura stramonium* plant (the Genus *datura* stems from the Hindi word *dhatura*: "plant," the species name *stramonium* is a compound word derived from two Greek terms: *strychnos*: "nightshade"– the common name for this plant – plus *manikos*: "mad, crazy" – thus *strychmanikos*, which has evolved into stramonium.) One of the common names for *Datura stramonium* is **Jimson Weed**, which derived its name from Jamestown, Virginia. In 1676, Nathaniel Bacon led an army of angry Virginia colonists against the governor of that colony, William Berkeley. The colonists were incensed over what they believed was Berkeley's ineptitude in protecting them from hostile Indian attacks. This uprising became known as **Bacon's Rebellion**, and was the first such revolt in U.S. history. A company of British soldiers was sent to subdue the insurgents, but unfortunately – and somewhat farcically – Jamestown weed (Jimson weed) had been accidentally added to a salad that the soldiers ate. In a book titled The *History and Present State of Virginia* (1705), author Robert Beverly described what happened next:

> *A very pleasant comedy, for they turned natural fools upon it for several days: one would blow up a feather in the air; another would dart straws at it with much fury; and another, stark naked, was sitting up in a corner like a monkey, grinning and making mows at them; a fourth would fondly kiss and paw his companions, and sneer in their faces with a countenance more antic than any in a Dutch droll.*
>
> *In this frantic condition they were confined, lest they should, in their folly, destroy themselves – though it was observed that all their actions were full of innocence and good nature. Indeed they were not very cleanly; for they would have wallowed in their own excrements, if they had not been prevented. A thousand such simple tricks they played, and after 11 days returned themselves again, not remembering anything that had passed.*[1]

Jimson Weed poisoning of domestic animals, such as horses, cows, sheep, etc. is a common problem across the United States. Upon ingestion the animal becomes restless, lethargic, ataxic, disoriented and salivates excessively. Thus another common name for this plant is **Locoweed**. (Loco is Spanish for "insane, crazy")

Let's return briefly to the Latin root tropos ("to turn"), which is also found in the words **tropics** and **tropical**. Our planet is tilted at an angle of 23.5 degrees from the sun's equator. On its annual circumnavigation of the sun, earth's **northern** hemisphere tilts 23.5 degrees away from the sun in winter, and 23.5 degrees toward the sun during summer. From our earthly perspective, it appears as if the sun is moving vertically up and down 47 degrees during the year – directly overhead at 23.5 degrees **north** of our equator on June 21st, then turning and moving to a position directly overhead at 23.5 degrees **south** of the equator on December 21st. These northern and southernmost points of the cycle (the latitudes where the sun appears to turn) are accordingly known as the **tropics** (the "turning" places). The lowest latitude (23.5 degrees south) is known as the Tropic of Capricorn (when the sun appears directly overhead at this latitude, the northern hemisphere experiences its winter solstice - occurring annually on December 21st or 22nd). The highest latitude (23.5 degrees north) is called the Tropic of Cancer (when the sun is directly overhead, the northern hemisphere experiences its summer solstice - on June 21st or 22nd).

On December 21st -22nd , the sun is 90 degrees above the horizon (directly overhead) in places located at 23.5 degrees south latitude, such as the Argentine Pampas, Alice Springs, Australia, the Kalahari Desert in Botswana, Sao Paulo, Brazil, the Atacama Desert of Chile, and Kruger National Park in South Africa. On June 21st -22nd , the sun is directly overhead at 23.5 degrees north latitude, in places such as Libya, Egypt, Saudi Arabia, the Gulf of Mexico and the Gulf of California. Unfortunately for American sun-worshippers, the southernmost city in our contiguous 48 states – Key West, Florida – is located at 24.5 degrees north latitude. Therefore, at **no** time during the year is the sun directly overhead (90 degrees) **anywhere** in the continental U.S.

When the sun reaches its lowest and highest points, it appears to **stop** moving for several days, then it turns and begins either its ascent or descent. These times are known as the winter and summer **solstice**. That term derives from Latin *sol*: "sun" and *sistere*: "to stop" – the sun literally appears to stop its vertical movement for a short while before turning and moving in the opposite direction. The word **armistice** has a similar derivation, meaning "a halt to arms or warfare."

It's a very nice word. It should be used more often.

Reference:

1. http://www.ansci.cornell.edu/plants/jimsonweed/jimsonweed.html

Barton J. Gershen, MD, Editor Emeritus of Maryland Medicine, *retired from medical practice in December, 2003. He specialized in cardiology and internal medicine in Rockville, Maryland.*

CLASSIFIEDS

LEASE/SUBLEASE/SALE

BETHESDA: Attractive office space for rent in physician's practice w/private office, exam rooms, and shared waiting room ready for use. Walking distance to Metro, parking garage, or on street and county garage across street. Please call Avelene at 301.656.0220.

FOREST HILL: Office space available in a quiet professional building. Includes utilities, phone, copy, fax machine, receptionist area, waiting room, and parking. Two examination rooms and all other necessary accommodations for an MD (sink, closets, file areas, etc.). Part-time availability (1-3 days a week). Please contact Dr. Schmitt at 443.617.0682 or Dr. Legum at 410.852.0582.

FREDERICK: Medical office space available to share. Approximately 2000 sq. ft., bright and modern office located at intersection of Guilford Rd. and New Design Dr. waiting room, front desk and physical therapy equipment available for use. Perfect space for an internal medicine/family practice looking to expand in the Frederick area. Hours of use and rent are negotiable. E-mail inquiries to hollyford@smartmed1.com.

GERMANTOWN: Medical office space for lease in Germantown. 4000 sq.ft., lots of free parking, easy terms. One block to New Holy Cross near Montgomery College, Germantown. Call 301.502.1833 or 301.515.6971 after 6 pm.

ROCKVILLE: 1,200 sq. ft. office next to Shady Grove Hospital. Available afternoons and weekends. 301.424.1904.

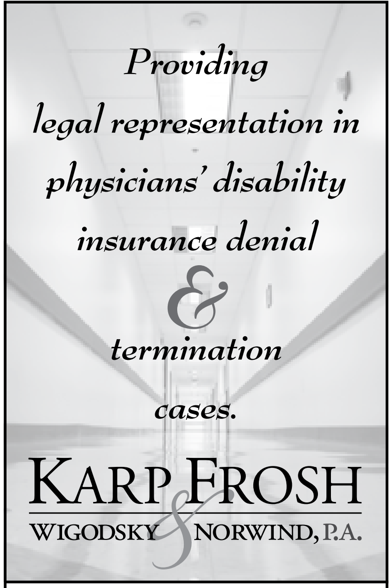
SILVER SPRING, DOCTORS MEDICAL PARK: Georgia Ave. at Medical Park Dr. Close to Holy Cross Hospital, ½ mile north of #495. 3 building medical campus totaling 95,000 sq.ft with over 100 practitioners and Clinical Radiology's HQ. 2 suites from 1100 sq.ft. avail. Call Steve Berlin at Berlin Real Estate, 301.983.2344 or steve@berlinre.com.

SILVER SPRING/WHEATON: Lower your overhead expenses by subleasing or sharing medical office space. Luxurious penthouse suite with 3200 square feet, 7 treatment rooms, surgery center, equipment and staff available. All medical specialties welcome. Call: 301.949.3668.

TOWSON: 2,087 square feet of second floor medical space available for lease at 660 Kenilworth Drive (directly across from Towson BMW). Suite is fitted for medical professional and landlord will build out to suit tenant's needs. Lease rate includes full utility and janitorial service. Attractive two story professional building with convenient and ample free parking. Caring on-site ownership and management. Excellent access to I-695, I-83, Timonium and downtown Baltimore. To discuss or see, call David Miller at 410.321.9558.

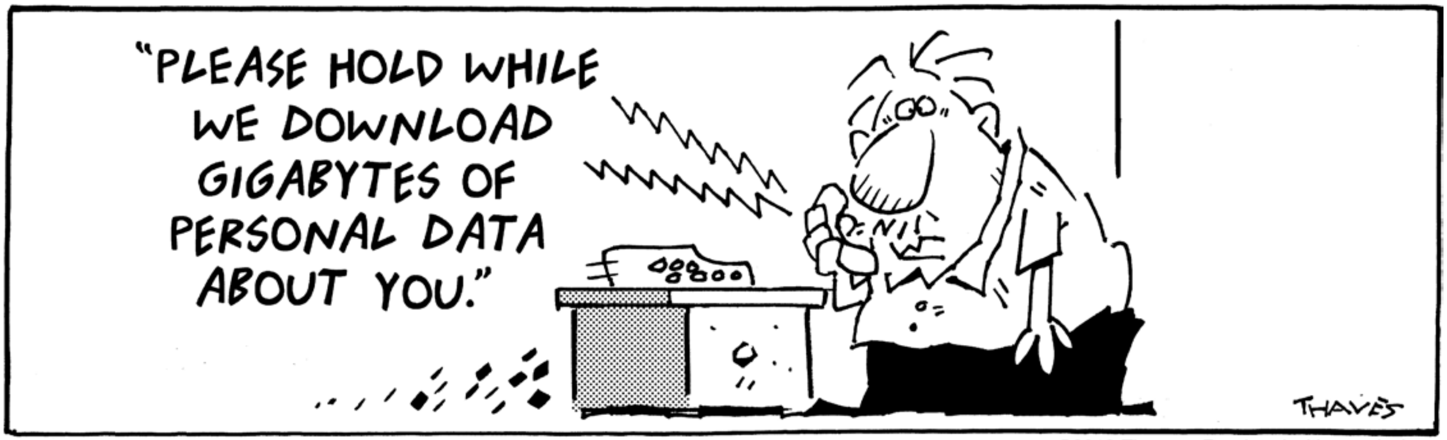
MEDICAL EQUIPMENT: Diomed Δ15 Laser (for vein closure), with angio-dynamic kits and pump, and Ritter-230 exam table. If interested, call 301.325.3212.

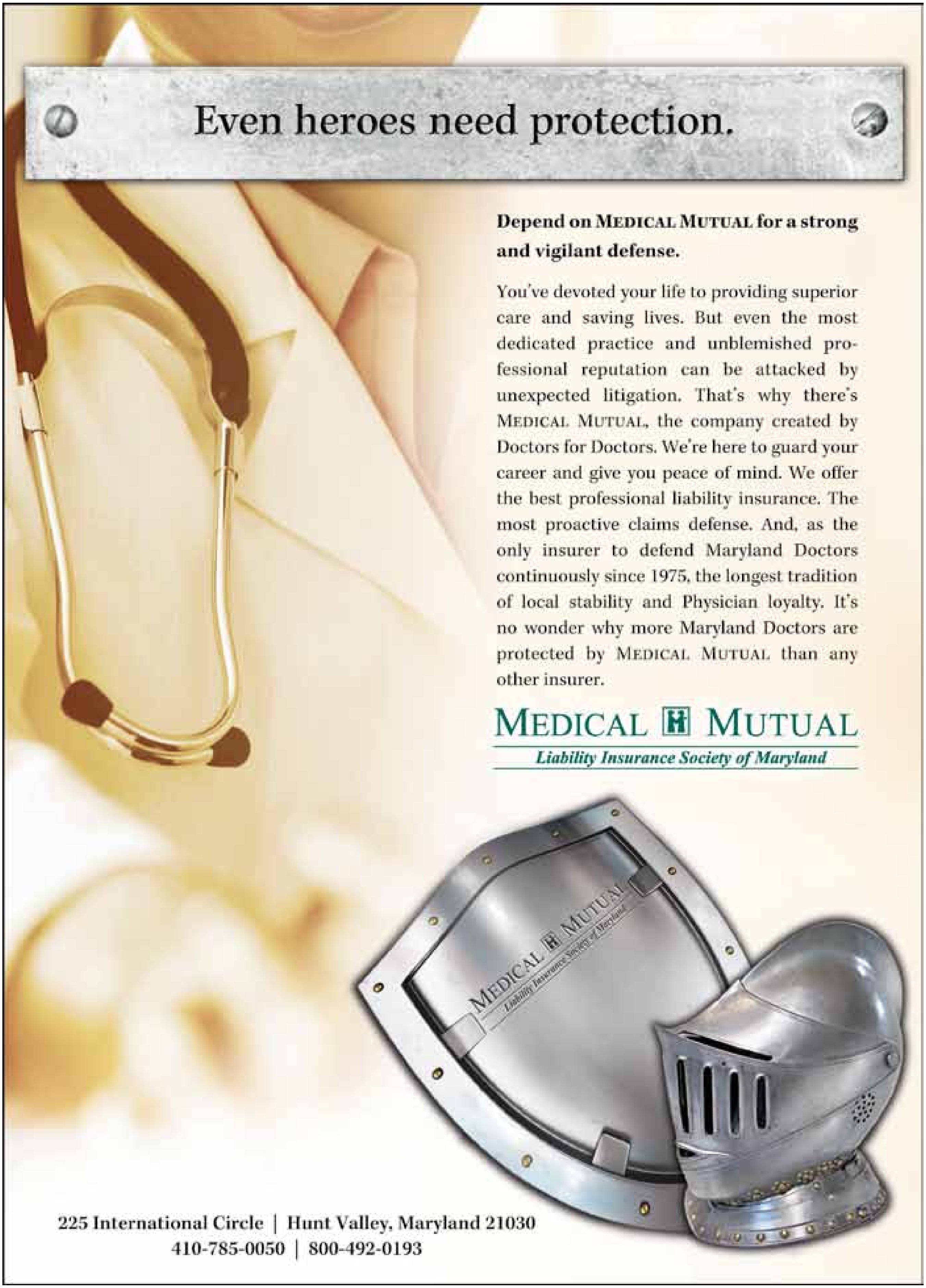
INTERNAL MD PRACTICE 4 SALE: 2 Exm Rms, Well-Staffed, 5K Charts, Call ProMed Financial 888-277-6633.



THE LAST WORD

Frank and Ernest


"PLEASE HOLD WHILE WE DOWNLOAD GIGABYTES OF PERSONAL DATA ABOUT YOU."
THAVES


Even heroes need protection.
MEDICAL MUTUAL
Liability Insurance Society of Maryland

MedChi
The Maryland State Medical Society

MedChi
The Maryland State Medical Society
1211 Cathedral St. ▯ Baltimore, MD 21201