April 2016

In this issue:

MSCI Newsflash

Security and Risk Assessment

Focus on HIPAA

Last year we witnessed a number of data breaches occur within hospital networks, health insurers, physician's offices and much more.

It's no secret, hackers are drawn to industries that hold valuable, sensitive and extremely personal data. Therefore, the healthcare industry has been a a main target for quite some time now. At risk, private information, demographics such as addresses, phone numbers; family histories, medical conditions, social security numbers.

Be prepared and protect your practice and your patients' PHI. Know what the proper safeguards are and acknowledge that risk does exist.

Here are a few steps toward getting your practice HIPAA compliant.

1. Educate your staff on the risks of sharing or exposing valuable data. Remind them that they too are responsible for keeping your data under virtual lock and key. Emails should never include a patient name or details about a patient's condition. Secure email is preferred. Have a standard HIPAA compliance agreement signed by each employee.
2. Make sure only the appropriate personnel have the access they should to such sensitive data as lab tests and results, patient diagnoses and other delicate information. Management and trusted clinical support staff should know to identify these things and access should only be given to staff members in the role of patient health representatives. User log-ins and access control must be stricter.
3. Make you network work for you. Your IT technician should be able to ensure your network is secure, that firewalls and encryption is in place. Technology can be your best tool in this digital world of medicine but make sure to use that technology to also protect the tools of your everyday job. Web security needs to be dramatically enhanced.
4. In the event of a data breach, it is essential to have an incident isolation and response plan ready. Make sure to have a recovery plan to ensure it doesn't happen again.
5. Have your Business Associates sign a confidentiality agreement, so you're protected from the inside and out.

Our goal is to minimize the risk of exposure of PHI and to eliminate the need for practices to ever have to report a breech in security.

MicroMD has a new logo!

MicroMD Training

Hired new employees? Need to explore more of your MicroMD? Want to know what secrets hide in the newest version release? MicroMD Training is always available at every level from brand new introductory lesson to advanced users and making your MicroMD work for you. We can tailor your lessons to your needs and your budget. Please let us know how we can help.

An Important Note About BAAs

Violation of the HIPAA Privacy and Security Rules can be very costly in many ways. Not only does it cost the patient their privacy and the risk of their data remaining secure, it can be very costly for your practice too.

A password protected laptop containing almost 9,500 PHIs, was stolen from a locked car which belonged to a business associate of a major hospital in Minnesota . There was no evidence that the thief accessed the personal and financial records stored on the laptop but it was discovered during an investigation that the hospital had never entered into a Business Associate Agreement with the employee of the company commissioned to handle their Revenue Cycle Management. It cost the hospital $1.5 million in fines.

- Don't share protected health information with a business associate without a valid business associate agreement
- Covered entities and business associates should perform HIPAA security risk assessments to uncover and address possible vulnerabilities.
- Electronic PHI should be safeguarded with encrypted technology. Portable devices are the easiest target for a breach in your security. Encryption will provide strong protection in case of theft.

There's A Code For That

T78.40 Allergy, Unspecified.

J30.1 Allergic Rhinitis Due to Pollen

J30.89 Allergic Rhinitis, Other Allergen

J01.90 Acute Sinusitis, Unspecified

L50.0 Allergic Urticaria

With the arrival of Spring comes allergies in many forms, unfortunately. For those who suffer from allergies brought on by the budding of trees or blossoming of flowers, or newly cut grass, it's never fun. Neither is trying to find the right ICD-10 code! There are tons of allergy related codes! Be sure you're using the right one.

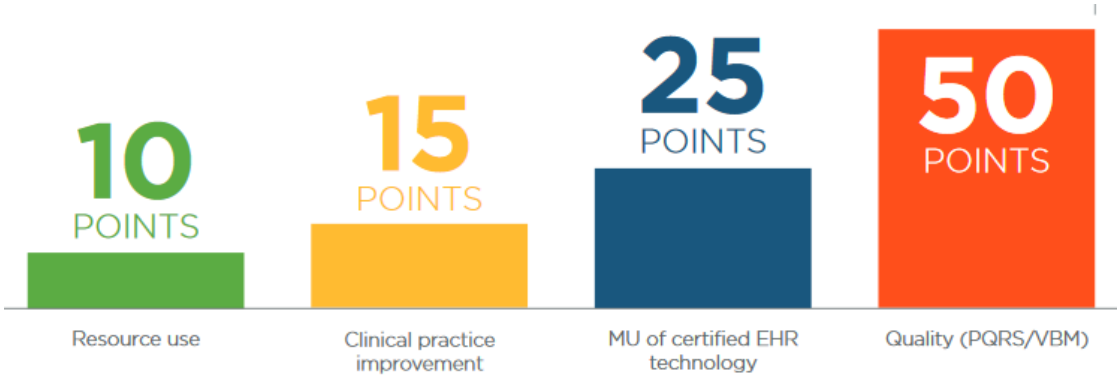
PREPARE FOR MIPS

Meaningful Use is not going away. Although initially it was a five year participation plan, it may seem like an end is near, Meaningful Use and PQRS (Physician's Quality Reporting System) are being combined into a new incentive program.

MIPS - Merit Based Incentive Payment System - is a consolidation of current incentive programs and a new one, all rolled into one. Starting in 2017, MIPS will annually measure Medicare Part B providers in four performance categories:

1. Meaningful use of an EHR system
2. VBM - Value Based Modifier quality based on PQRS
3. VBM cost or resource use performance
4. Clinical Practice Improvement.

Providers will be rated on a points system, each of the four categories having a maximum point value and a minimum Performance Threshold (PT). Those providers meeting the PT will not be assessed a penalty. For scoring under the PT penalties will be incurred. And for those exceeding the PT, an incentive will be awarded.



Who's eligible for MIPS?

EPs beginning 2017:

- Physicians, physician assistants, nurse practitioners, clinical nurse specialists and nurse anesthetists.

EPs added in 2019:

- Physical or Occupational therapists, speech-language pathologists, audiologists, nurse midwives, clinical social workers, clinical psychologists, and dietitians or nutrition professionals.

Who's exempt?

- Providers not meeting "low volume threshold".
- MSSP ACO providers and other participants in "alternative payment models".
- First-year Medicare providers.

*Medix is currently checking with HSMS regarding the plans they have for assisting practitioners with tracking scores for MIPs, and will keep you posted of any new information.

Is there an alternative to MIPs?

APMs give us new ways to pay health care providers for the care they give Medicare beneficiaries. For example:

- From 2019-2024, pay some participating health care providers a lump-sum incentive payment.
- Increased transparency of physician-focused payment models.
- Starting in 2026, offers some participating health care providers higher annual payments.

Accountable Care Organizations (ACOs), Patient Centered Medical Homes, and bundled payment models are some examples of APMs.

"Qualifying APM participants" will not be subject to MIPS adjustments and will receive a lump sum incentive payment equal to 5 percent of the prior year's estimated aggregate expenditures under the fee schedule. The 5 percent incentive payment is available from 2019 to 2024, but beginning in 2026, the fee schedule growth rate will be higher for qualifying APM participants than for other practitioners.

New CMS Primary-Care Payment Model

Although it has not been decided yet if this will also be an alternative to MIPs, the CMS is planning another reimbursement in the form of a monthly fee, to practices that will participate in their new plan to manage care for as many as 25 million patients in an effort to transform and improve how primary care is delivered and reimbursed to the provider.

The Comprehensive Primary Care Plus initiative will include up to 5,000 practices nationwide involving more than 20.000 practitioners. The program is designed to collaborate with commercial, state and other federal insurance plans.

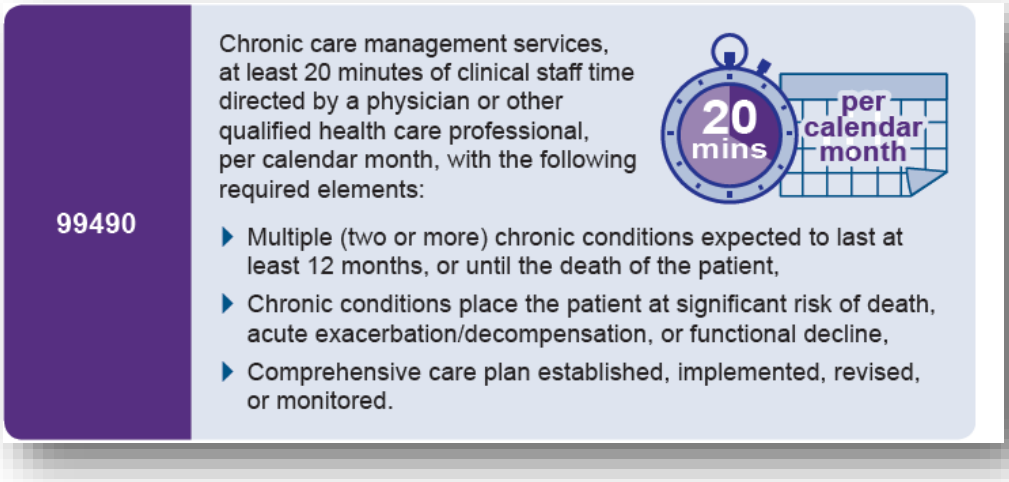
The regions in which this CPCP initiative will take place have not yet been determined but when it is rolled out, participants will be able to choose from two ways to participate.

Track 1: ($15 per month per beneficiary)
Practices are paid an monthly fee for providing specific services. That fee is in addition to the fee-for-service payments under the Medicare Physician Fee Schedule.

Track 2: ($28 per month pre beneficiary)
Practices will receive a monthly care management fee and instead of full Medicare fee-for-services payments, they will receive reduced Medicare FFS payments and up-front comprehensive primary-care payments. This hybrid payment design will allow greater flexibility in how practices deliver care outside of the traditional face-to-face encounter.

Low performance on quality and utilization of EHR may require that providers would have to pay back any up-front payments. However, feedback has been somewhat positive in that it will allow practitioners to focus more office time on the chronic and ailing patients and accommodate the exploration of telemedicine based practice for those in less of a need.

Chronic Care Management (CCM) is defined as the non-face-to-face services provided to Medicare beneficiaries who have multiple (two or more), significant **chronic** conditions.



MSCI has a partner company that can assist physicians to improve their care delivery to clients with chronic illnesses by providing Centers for Medicare & Medicaid Services (CMS) reimbursable services to Medicare patients with two or more CMS eligible chronic conditions. Chronic Care Managers provide a minimum of twenty (20) minutes of telephonic care/case management support per month to each Medicare patient enrolled in the program. Contact MSCI to find out how we can help you.

RANSOMWARE

You may have heard of it, but if you haven't, you're going to want to know. Grouped as ransomware, they come in many names including several identifying themselves as FBI related. Logo and all. It is usually an ordinary email with an unsuspicious subject like "invoice" or "update" that is invited into your system by a simple unsuspecting click.

But once it's opened, you have unleashed a powerful virus that holds your hard drive hostage and can very easily creep through and infect other workstations on your network including your server.

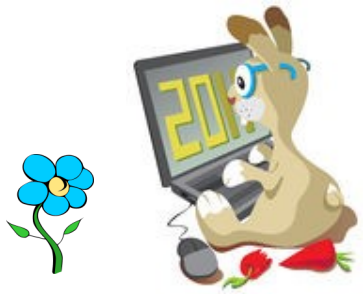
If you're lucky enough to catch it before it spreads to other systems, disconnecting the infected hardware from the network is the first step. The virus kindly provides detailed instructions via pop up messages on how to retrieve the key to unlock the files it is holding captive. And that's where the tag 'ransomware' comes in.

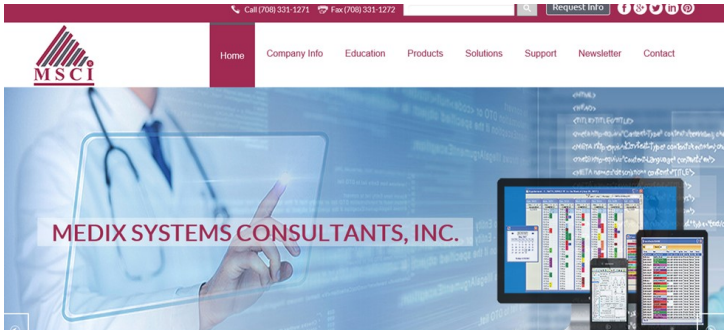
Your files, applications and other functions of your system are frozen and rendered inaccessible until you follow the instructions on the pop-up and pay to have them unlocked. In the meantime, you can't use your EHR (paper charting!), you can't use email and it's likely you won't be able to access any documentation saved on your computer.

What can you do to protect yourself and your hardware?

Tune in to the MSCI Webinar on Wednesday April 20th to hear about ransomware and what you can do to avoid the costly virus.

Medix Systems Consultants, Inc.





MSCI Monthly EMR User Forum
Registration Link Below

Join us for our PM Webinar
Wednesday April 13, 2016
at 10:00 AM CST.
Register now!
https://attendee.gotowebinar.com/register/2993459263076814595
Reminder: The deadline for user submitted questions is 4/6/2016!

And..

Join us again for our EMR Webinar
Wednesday April 20, 2016
at 10:00 AM CST.
Register now
https://attendee.gotowebinar.com/register/6123254295913272323
Reminder: The deadline for user submitted questions is 4/13/2016!

After registering, you will receive a confirmation email containing information about joining the webinar.

GoToWebinar by CITRIX

Like our website?
MSCI is proud to offer web design and maintenance as one of our specialty services. Give your website a fresh new look for Spring, or have a brand new website developed by our experienced web-designers. Contact us today for more

Our address is:
600 Holiday Plaza Drive
Suite 545
Matteson, IL 60443

Ph: 708-331-1271
Fax: 708-331-1272
Email: Support@imsci.com
Website: www.imsci.com

MSCI

"SOLUTIONS FOR THE FUTURE... TODAY"