



IN THIS ISSUE:

5010 is coming...
What you need
to know [Page 1](#)

Outsourcing
Strategies to Achieve
Meaningful Use
[Page 1](#)

Free eRisk
Seminar Series
See the schedule
[Page 2,3](#)

FAQ:
Meaningful Use
[Page 3](#)

Tips for Securing
Your Mobile
Devices [Page 5](#)

5010 is coming... What you need to know

Beginning January 1, 2012, all healthcare providers will be required to submit claims using the new 5010 format. Will you be ready in time?

For the last several years we've been using the 4010A1 set of the HIPAA electronic transaction standards. These standards apply to all professional and institutional claims, as well as ERAs, claim acknowledgments and claim status transactions, and affect providers, payers, clearinghouses and software vendors.

But that will change on Jan. 1, 2012, when we are required to begin using the new 5010 format.

If you're using NextGen, you will need to upgrade to Version 5.6 SP1 to begin submitting claims in the new format (this includes the errata). If you have not done so, be sure to upgrade your test environment so you can begin initial testing with your clearinghouse.

Continued on Page 4

Outsourcing Strategies to Achieve Meaningful Use

At the very basic level of meaningful use (MU), clinics need to go electronic to support MU objectives, which are evident in both the core and menu sets of MU. But, regardless of MU and standards set by HIPAA security, the implementation of EHR and its impact on patient care requires more sophisticated, responsive and stable systems and networks. Going electronic is an expensive and resource-intensive process. For those that haven't started, the task can be daunting.

So how do you begin, and when does it make sense to outsource?

According to a report by the Medical Group Management Association, the average multispecialty practice spends approximately 1.5 percent of its total medical revenue on IT costs. While hospital-owned practices generally have the advantage of access to resources through hospital information technology (IT) staff, independent practices must turn to more practical options, such as outsourcing, to manage their basic IT needs.

The options between what to staff and what to outsource are plenty. So how should a practice approach a decision to invest in its

Continued on Page 2



Join us for these free webinars, or watch and listen on the MMIC Health IT website.

For registration, dates and information on upcoming MMIC webinars go to MMICHealthIT.com/webinars.

eCommunication with Patients

9/21/2011, Noon – 1 pm

Following this webinar participants will be able to:

- Understand how communication breakdowns are a leading cause of patient injury and malpractice claims
- Utilize the latest electronic methods to enhance patient communication, provider collaboration and customer satisfaction
- Identify strategies to minimize the risks involved in electronic communications and social media

Making eCommunication Meaningful and Secure

10/19/2011, Noon – 1 pm

Both physicians and patients can benefit as practices adopt new internet communications – and the options are growing:

- How do you know which ones will help your practice achieve Meaningful Use?
- How can you be sure patients' protected health information is delivered securely?

This webinar will address these issues and look at different types of eCommunication.

Electronic Discovery

11/16/2011, Noon – 1 pm

This webinar will review:

- The basic principles of electronic discovery
- The importance of a properly executed litigation hold
- The importance of an appropriately administered document retention plan

own technology and staff vs. outsource IT resources? While there's no one-size-fits-all answer, there are a few key areas that can help point to the right solution for your practice.

One approach is to first determine your goals, assess your risks, identify your needs and perform a gap analysis. Urgency increases the need for higher availability of patient data, security over networks and disaster recovery strategies to be in place.

Most practices, regardless of size, will employ some combination of outsourcing depending on the knowledge level or workload strain of the internal staff.

The biggest factors in determining staffing-to-outsourcing ratios are the size of practice and its technology philosophy. The size of the practice inputs includes the number of providers, the amount of staff to support and the total medical revenue. The philosophy on technology is more subjective and refers to the values of the leadership within the practices, their comfort level around technology and the ability to manage change. Does the leadership shy away from computerized systems or do they embrace technology and create excitement around its advantages?

Typically, the more progressive a practice is with technology, the higher its IT staff-to-user ratio. For example, high-tech practices, which depend on more complex computerized systems—such as EHR, practice management, accounting, digital imaging and radiology systems, wireless environments, unified

messaging, secure email, various lab systems and clinical devices—tend to have a ratio closer to 1:25 to 1:50 IT staff to users. The IT staff structure will include an IT manager with a team of support staff.

Most practices have philosophies that fall in the range of IT with “full service and overall value” at a ratio of 1:60 to 1:100 IT staff to users. Practices with this philosophy will tend to have practice management systems, maybe an HER and peripheral diagnostic systems.

All sizes of practices, depending on how knowledgeable or strained for capacity a staff is, will employ some combination of outsourcing. Most practices with fewer than 100 users typically outsource all of their IT resources. IT vendor coordination usually falls onto the list of responsibilities of an office manager or business office supervisor. Practices that choose to keep their IT under closer control will more likely employ staff rather than outsource. Practices with 100 to 200 staff members will employ an IT generalist who also coordinates outsourced network specialists. Larger practices usually have an IT team with an IT manager and team of support staff. But because of the vast and increasing amounts of knowledge needed to support computer systems with today's technology, it is difficult to encompass all the specialized skills within an individual person or a small team. Therefore, even larger practices will outsource the specialized skills for their more complex systems and devices.

Practices may choose to outsource their complete IT support through managed services, which may include help desk as well as PC and server maintenance. Gartner reported up to a 42% savings on managed PCs. Backups and disaster recovery are also becoming offered as a managed service, offloading the need for staff to manage server backup.

Continued on Page 3

Practices can also choose to lease printers, computers and servers to avoid hardware obsolescence, which usually translates into support. Practices can choose to deploy their own "thin" environments where all processing is done on a server, minimizing the need for hands-on help desk support, as opposed to "thick" or "fat" environments where all applications are installed locally.

Outsourcing options also continue to grow as Internet technologies improve, available bandwidth for transferring data increases and cost for added telecommunications and data lines decrease. Some practices choose to have their systems hosted for a fixed fee through an Application Service Provider (ASP)

model in which the ASP is responsible for keeping their systems maintained, secured and backed up. And practices can also partake in a completely hosted enterprise environment, where the majority of support and maintenance is done via a third party with Service Level Agreements (SLA) in place.

To choose the right combination for your practice, the best place to start is by defining your technology philosophy and goals based on a best practices budget percentage. Then get help. MMIC Health IT can help you to get to Meaningful Use by helping you assess your risks, identify your needs, analyze cost scenarios, interview staff and assist with vendor and system selection.

FAQ: Meaningful Use

Q: Will we have to report on more than just our Medicare/Medicaid population?

A: Yes. The requirements necessary to meet measurements are based on the practice's entire patient population, regardless of whether it chooses to submit for incentives through Medicare or Medicaid.

Q: Do eligible providers need to choose between the Medicare and Medicaid programs?

A: Yes. Each practice must choose (not at the eligible provider level) whether to participate in either the Medicare or Medicaid program each year. In addition, practices choosing to report under Medicaid must be re-qualified each year of participation.

Q: Are mid-level providers considered eligible providers?

A: No. The definition of eligible provider is: The term "physician," when used in connection with the performance of any function or action, means (1) a doctor of medicine or osteopathy

legally authorized to practice medicine and surgery by the state in which he performs such function or action. The following are also named as eligible professionals: doctor of dental surgery or medicine, doctor of podiatric medicine, doctor of optometry and chiropractor.

Under the Medicaid program (42 USCS § 1396b), the term, eligible professional means a physician; dentist; certified nurse mid-wife; nurse practitioner; and physician assistant in so far as the assistant is practicing in a rural health clinic.

Q: Should practices that do not qualify as eligible providers still be concerned about being on a certified system?

A: Yes, even if it is not mandatory. Working on a system that meets MU certification will allow for interoperability and carry additional benefits that should help the practice improve the care it provides.

Join us for these free webinars, or watch and listen on the MMIC Health IT website.

For registration, dates and information on upcoming MMIC webinars go to MMICHealthIT.com/webinars.

CPOE Issues: Implementing Computerized Physician Order Entry (CPOE) November 9, 2011

In this webinar, a panel of experts will discuss the perspectives of key stakeholders (IT vendors, physicians, support staff and organizational leaders) to identify common barriers and solutions to CPOE.

Discovering ESI December 2011

Do you know where your data is? With the adoption of electronic health records, tablets, smart phones, and other portable devices, healthcare organizations must be progressively more prepared for electronic discovery.

This webinar will raise technical awareness of the different forms of media that contain other discoverable electronically stored information (ESI).



5010 is coming... What you need to know

Continued from Page 1

Below are some actions you can take to prepare for this change. You'll want to take these actions before you install Version 5.6 in your test environment. Then have your production database copied into test when Version 5.6 is loaded. This way you will not have to make these changes for the testing process and then repeat them in the production database when you upgrade to Version 5.6 live. Before making any of these changes, be sure to check with your clearinghouse and payers to make sure these changes will not cause issues with your current 4010A1 billing.

- **Billing Provider NPI subparts.** If you have NPI subparts, make sure you have them clearly defined and correctly entered in file maintenance. The subpart reported as the Billing Provider must be at the most-detailed level of enumeration.
- **Individual Providers.** In 5010, the Billing Provider can only be an individual when the services are performed by an independent, non-incorporated provider.
- **Billing Provider Address.** The Billing Provider address can no longer be a post office box or lock box. It must be the physical address associated with the NPI subpart. If you have a lock box or P.O. Box, you will still have it in the address in the Group-Payer records, but you will also need to select a location that will be used to pull the Billing Provider address. When it is set up this way, electronic claims send the Group-Payer address in the "Pay To" loop and the address of the location you select in the "Billing Provider" loop.
- **Nine-digit ZIP code.** 5010 requires a nine digit ZIP code for the Billing Provider Physical Address and for Service Location

addresses. Review your Group Master List and Location Master File to make sure these codes have been entered. There will be a claim edit in Version 5.6 to flag any you might miss.

- **Place of Service = Home (12).** In 5010, the patient's address will replace the service location address whenever the Place of Service is set to "Home." For this reason you may want to begin capturing the full nine digit zip code for patients who routinely have services provided in the home.
- **Service/Facility Location NPIs.** You should **not** report the NPI for your internal service locations; however, you **must** report the NPI for external/facility locations, such as hospitals, nursing homes, rehab centers, etc. Review your Location Master File and make sure it meets these requirements.
- **Pending Claim Requests.** You may have some outstanding pending claim requests that are not marked for processing and thus are not being sent. You will want to review these claims and make sure all of them are at least marked for processing so they will be updated to the correct submitter profile when you make the change. If they are not marked for processing, the submitter profile library change will not flow to them.
- **Provider Secondary References.** Clean up any references to legacy identifiers that are not used anymore (e.g., 1B, 1C, 1D, etc.). As of 5010 only the EI/TaxID should be sent for the Billing Provider.
- **Release of Information.** In the future, the only valid options will be "Y" or "I." You can use the "A" because it will be mapped to "Y" in Version 5.6. Any other options will be kicked out as invalid by a claim edit.



Contact us!

For all inquiries other than support, email us:
info@mmichealthit.com

Or call us at:
877-838-6869

Current Clients:

To access our client support center:

Phone:
952-838-6868

Toll Free:
888-928-8266

Fax:
952-843-2100

E-mail:
ClientSupport
@MMICGroup.com

Continued on Page 5

Need more information? Visit us at www.MMICHealthIT.com or email us at info@MMICHealthIT.com

Once you have your test system set up in Version 5.6, contact your clearinghouse to find out if they are ready to test and what actions you need to take. Initial testing can be done from your test system. Once the clearinghouse testing is complete, you will need to test with individual payers as they come online with the 5010 format. Your clearinghouse can keep you informed on which payers are ready for testing. You can test them from your Test environment or in your live environment. We suggest that you have two submitter profiles, one for each format. As payers go live on 5010 and you complete testing, be sure to move those payers onto the new submitter profile.



We will have resources available on the MMIC Health IT Resource Center to assist you with this change. In addition, there are many additional resources available at the NextGen website, through clearinghouses and through CMS, including:

CMS: www.cms.gov/Versions5010andD0

GetReady5010: www.getready5010.org

NextGen: www.nextgen.com

White papers

Training opportunities (announced in "What's Next" newsletter)

Monthly 5010 claims webinar

Ask5010@NextGen.com

Gateway EDI: www.gatewayedi.com/5010
industryinfo@gatewayedi.com

Navicare: www.Navicare.com

If you have questions about any of this information, contact the MMIC Health IT Client Support Center at 952-838-6868 or toll-free at 1-888-928-8266 or email ClientSupport@MMICGroup.com.

To access our client support center:

Phone:
952-838-6868

Toll Free:
888-928-8266

Fax:
952-843-2100

E-mail:
ClientSupport@MMICGroup.com

Tips for Securing Your Mobile Devices

As cell phones and PDAs have morphed from simple phones and calendars into miniature computers, we're increasingly relying on them to navigate both our work and personal lives. In many cases, people use their personal phones to view work-related emails. While this may increase efficiency, it can put your patient data at risk and potentially subject you and your company to legal liability.

In the past, most malicious software was written by people seeking to cause mischief and mayhem. Now most malware is created to steal data for profit or to use your services without your knowledge. Most cell phones today are miniature computers—and they are

increasingly under attack. In one recent case, a researcher at Veracode, a mobile software security company, created spyware for a mobile device that could harvest data he could cross-reference against other hacked databases to determine the cell phone user's location, personal information and business relationships. Others have created programs that will, without the user knowing, turn on the phone's microphone to record a call and email the call to a predetermined email address.

Continued on Page 6





7701 France Avenue South,
Suite 500
Minneapolis, MN 55435



Tips for Securing Your Mobile Devices *Continued from Page 5*

While there is no foolproof way to protect your mobile devices, there are ways to help protect your patients, yourself and your business from compromising private data:

- Have a well-crafted cell phone and PDA policy. Your IT provider should be able to help you draft a policy to protect your patients' and your company's data.
- Insist on password protection. You may even be able to have the phone wipe itself of all data if the wrong password is tried too many times in a row.
- Use encryption. With it, lost or stolen phones can be remotely wiped clean using various tools. A 16 gigabyte phone can contain a lot of patient and company data that you do not want in the wrong hands.
- Stay up-to-date on operating system patches. These patches are specifically designed to repair security vulnerabilities.
- Purchase mobile anti-virus software for your phone and keep it up-to-date.
- Be careful about posting your cell phone number and email address. This information can be used as a point of attack on your computer or to attempt to lure you to a site that will try to compromise your phone. If you receive emails and texts that contain links, be wary and do not follow the links to the website.
- Be wary of downloads. Many sites offer games and software for download; sometimes they contain malicious code. If you receive files from a website, look for a web site security certificate.
- Be educated on phishing. From Twitter to MySpace to Facebook and any other social network site, email or text, do not put personal information, cell number, passwords or personal information into a site that you didn't browse to directly yourself and verified it has a proper certificate. Be cautious and verify a company's website and/or phone number.
- Watch your Bluetooth. While Bluetooth is a great connectivity tool, it also can establish connections to other phones and devices that you don't want to connect to. Many viruses exist to make use of the default-on features. Make sure your Bluetooth is set to connect only to the devices you set up.
- Be wary of open Wi-Fi networks. Transmissions on public Wi-Fi networks are highly vulnerable to eavesdropping.

Be sure to work with your IT department or technology consultant to formulate policies and obtain technologies to protect your critical patient health information and other business data.