The new ICD-10 implementation date is less than a year away, and CMS is gearing up its end-to-end testing process in preparation.

CMS will select submissions from approximately 2,550 volunteers for three separate testing opportunities in January, April, and July 2015 and will make an effort to choose participants that represent a variety of provider, claim, and submitter types. MLN Matters SE1409 Revised (www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNMattersArticles/Downloads/SE1409.pdf) states that the goal of the testing is to demonstrate the following:

- Providers or submitters are able to successfully submit claims containing ICD-10 codes to the Medicare fee-for-service claims systems
- CMS software changes made to support ICD-10 result in appropriately adjudicated claims (based on the pricing data used for testing purposes)
- Accurate remittance advice is produced

Take action as early as possible regardless of whether your organization opts to test with CMS or another payer, says Barbara Hinkle-Azzara, RHIA, vice president of HIM operations at HRS Coding in Baltimore. Throughout the transition to ICD-10, organizations have made the mistake of assuming they will be able to test with payers only to find themselves left in the dark because payers are only testing with a limited number of providers, she says.

In addition to end-to-end testing, CMS’s four-pronged approach to ICD-10 testing involves testing its systems, examining provider-initiated beta testing tools, and acknowledgement testing. Providers, suppliers, billing companies, and clearinghouses are welcome to submit acknowledgement test claims to CMS at any time until October 1, 2015. CMS will schedule acknowledgement test weeks in November 2014, March 2015, and June 2015, at which time all Medicare Administrative Contractor (MAC) and Common Electronic Data Interchange contractor help desk lines will be open to answer
questions about test claims.

Although this testing is relatively informal, participants will still receive MAC acknowledgement about whether their claims were accepted or rejected. Participating in this type of testing may be a good indicator of whether your organization is on track with coding claims in ICD-10 even though it will not produce payment information, Hinkle-Azzara says.

Develop a process

Volunteering for CMS’ ICD-10 end-to-end testing is just the tip of the iceberg. Even if your organization is unable to participate in one of the CMS opportunities, make an effort to test with other payers so you know how the transition may affect your revenue stream and workflow come October 1, 2015. Consider the following as you embark upon ICD-10 end-to-end testing efforts:

- Pull your team together. Selecting cases for testing requires a great deal of thought and analytics. A group effort is required to ensure the testing process is as seamless as possible, says Wendy Coplan-Gould, RHIA, president and CEO of HRS Coding.

HIM professionals should collaborate with their revenue cycle and IT colleagues when considering ICD-10 end-to-end testing. This will be especially helpful when it comes time to produce the test claims through dual coding. “HIM needs to be at the center, leading this call for data analytics,” Coplan-Gould says.

Typically, a revenue cycle professional working in patient accounts or billing will be the primary contact person for payers throughout testing, and HIM professionals should assist in this process to the best of their abilities, Hinkle-Azzara says.

- Communicate with payers. Internal collaboration is essential to a successful transition to ICD-10, but so too is external collaboration. Once you’ve pulled your key players together, start communicating with payers. If you are unsure of what a payer needs to successfully test with your organization, just ask, Hinkle-Azzara says. “A lot of the payers—particularly as a result of the delay—seem like they’re going to be more open to collaboration and dialogue,” she says.

Develop a process

Volunteering for CMS’ ICD-10 end-to-end testing is just the tip of the iceberg. Even if your organization is unable to participate in one of the CMS opportunities, make an effort to test with other payers so you know how the transition may affect your revenue stream and workflow come October 1, 2015. Consider the following as you embark upon ICD-10 end-to-end testing efforts:

- Pull your team together. Selecting cases for testing requires a great deal of thought and analytics. A group effort is required to ensure the testing process is as seamless as possible, says Wendy Coplan-Gould, RHIA, president and CEO of HRS Coding.

HIM professionals should collaborate with their revenue cycle and IT colleagues when considering ICD-10 end-to-end testing. This will be especially helpful when it comes time to produce the test claims through dual coding. “HIM needs to be at the center, leading this call for data analytics,” Coplan-Gould says.

Typically, a revenue cycle professional working in patient accounts or billing will be the primary contact person for payers throughout testing, and HIM professionals should assist in this process to the best of their abilities, Hinkle-Azzara says.

- Communicate with payers. Internal collaboration is essential to a successful transition to ICD-10, but so too is external collaboration. Once you’ve pulled your key players together, start communicating with payers. If you are unsure of what a payer needs to successfully test with your organization, just ask, Hinkle-Azzara says. “A lot of the payers—particularly as a result of the delay—seem like they’re going to be more open to collaboration and dialogue,” she says.
Hinkle-Azzara and Coplan-Gould recommend that organizations look at their top 10 payers and select three to five with which to test their cases. When considering which payers to work with, reflect on your 5010 electronic data interchange experience to identify those who lagged behind in their readiness to process claims using 5010, says Rose Dunn, MBA, RHIA, CPA, FACHE, FHFMA, chief operating officer and founder of First Class Solutions in St. Louis and an MRB editorial advisory board member. “These will be the 20% of your payers that may cause you 80% of your problems with ICD-10 claim submission,” Dunn adds.

Ask each payer whether they are testing with a mapping tool or ICD-10 codes loaded into their system. If the information is loaded, then the ICD-9 and ICD-10 codes should be matched one-to-one in the payer’s system, at which point the payer will then accept or deny the claims. Alternatively, the payer may use General Equivalence Mappings (GEM) to map the ICD-10 codes back to ICD-9 before determining whether they are accurate and payable, Coplan-Gould says. “Some are testing with the native ICD-10 coding and getting real results, and some are able to accept the ICD-10 codes, but they may plan to map them back using the GEMs and then they pay based on where that ICD-10 code mapped, and that’s really not going to tell you that your claim is coded correctly or paid correctly,” she says.

Hinkle-Azzara agrees that GEMs may not give organizations all of the information they need to prepare for ICD-10. Mapping does not guarantee that the ICD-10 code that offers the greatest specificity will make it onto the claim. Take advantage of ICD-10’s options and instruct coders to review records and select a code that offers as much detail about the patient as possible. “From a testing perspective, who wouldn’t want to be able to say that the claim information contains that specificity?” Hinkle-Azzara says.

- Select the right case mix. Do your research before preparing for an ICD-10 testing opportunity with CMS or another payer. Dual coding records for end-to-end testing submission is a difficult task, and organizations should plan ahead to ensure they are on the same page as the payer when it comes to selecting records for testing. “There were providers that requested to test with their payers and they were denied,” Hinkle-Azzara says. “Additionally, some of the payers are actually selecting what cases they want to test.”

Although CMS remains tight-lipped about certain details of its ICD-10 testing program, the idea that some payers may test with organizations based on a standard case mix may not work well for all participants, Coplan-Gould says. “If the payers are selecting certain cases across the board, those cases really may not give you the type of information you hope to glean from the end-to-end testing,” she says.

Ensure that the payers with which you test understand the needs of your organization. Just because a payer has its mind set on gathering a certain case mix from your organization doesn’t mean the analytics produced from this testing will be of the most value to you, Coplan-Gould says. “Negotiate with the payer and select other cases that may be of benefit and of interest to your facility,” she says.

To determine which case types may be the most beneficial for your organization to test, start by looking at the codes that Recovery Auditors may have targeted at your organization as well as your high-volume DRGs to determine which codes your organization should test, Hinkle-Azzara says. “Where do you have cases that have been identified for audits in the past?” she says. “Those are the things we would recommend.”

Selecting cases for testing in this manner can be helpful, but Coplan-Gould reminds organizations to explore all potential areas of weakness when selecting cases that are suitable for testing. Examine physician documentation to determine whether your top diagnoses and procedures can map from ICD-9 to ICD-10 and result in accurate reimbursement for services based on information currently in the record, she says.

“If you are unsuccessful in budging the payer to incorporate certain claims in the mix, study the claim types that the payer chose,” Dunn says. For example, payers may be inclined to test claims that represent gray areas where coding is left to the coder’s discretion, such as two principal diagnoses present on admission with one possibly resulting in a higher DRG. This scenario often results in the payer adjusting the sequencing so the principal diagnosis is the lower-paying DRG, she adds.

Be flexible. End-to-end testing should be mutually beneficial. Although it is important to understand the cases of greatest testing value to your organization, you also need to take direction from payers when necessary.
“They key is not to go in assuming that you can tell the payer what to test,” Hinkle-Azzara says. “You have to be able to work with them.”

- **Prepare claims for testing.** Once an organization has selected payers with which to test and determined how many cases to submit, it’s time to start producing ICD-10 claims. Dual coding records in ICD-9 and ICD-10 may benefit organizations in several ways. In addition to being a great training exercise and identifying holes in current physician documentation, it is typically a good method for preparing claims for end-to-end testing, Hinkle-Azzara says. Using the identified case mix, coders should begin natively coding claims in ICD-10 so they can be submitted for testing.

“To get the most out of the dual coding practice, the coders should use their books, not their encoders, to ensure that the coder understands the ICD-10 coding guidelines and selects specific codes based on the documentation,” Dunn says.

Don’t forget to validate ICD-9 coding and DRG assignment prior to starting the dual coding process.

“There are still problems that people have with their ICD-9 coding, so it’s important to validate the coding of those test cases to begin with so you know what your baseline is,” Hinkle-Azzara says. If the original ICD-9 codes on your organization’s claims were incorrect, this will need to be addressed prior to coding the claims in ICD-10 and submitting the data for testing.

Check ICD-10 codes as well for accuracy before submitting test claims, Hinkle-Azzara says. Although electronic dual coding is recommended and can reduce errors, organizations may opt for manual coding. Because the format of ICD-9 and ICD-10 codes is so different, it can be relatively easy for a coder to make a mistake by doing something as simple as transposing an “O” instead of a zero. “Believe it or not, we’ve seen issues with that,” Hinkle-Azzara says. “The claims bounce back because they either have transposition or typo errors.”

In addition, consider throwing a curveball at a payer, Dunn says. For example, submit a claim with obvious errors, such as an ICD-10-CM code that begins with a number or an ICD-10-PCS code with six characters instead of seven, she says. This confirms that the payer adjusted the system edits for these issues and that the provider will be promptly notified to correct the edit and resubmit the claim.

“These same claims should ‘kick out’ from the patient accounts billing system edits before they go to the payer,” Dunn says. “Testing both separately checks your system’s readiness as well as the payer’s readiness.”

- **Don’t be afraid to ask for help.** Bringing in backfill coders may be helpful for organizations looking to stay on top of their daily routine while producing dual coded claims for testing. “Identify how much you want to dual code, how many hours you want to have your team committing, and then look at what kind of gap you need to fill,” Hinkle-Azzara says.

Consultants can often help ensure ICD-9 codes are correct before coders begin swapping them out for ICD-10 codes and can later review the dual coded claims. If your organization goes this route, consider dropping the selected claims into your release of information vendor’s website rather than granting the consultant permission to connect directly to your EHR, Coplan-Gould says. A control list that details which records will be placed in the queue is recommended to ensure all records are included and none are duplicated, she says.

**Gaining momentum**

The news that October 1, 2014, would no longer be the “go live” date for ICD-10 may have deterred some providers and payers from maintaining the same sense of urgency surrounding their implementation plans. Some organizations may have allowed their ICD-10 committee to take a breather, while others stayed on track with their timeline, Hinkle-Azzara says. “We’ve heard sort of a mixed bag,” she says. “But the key is to get that dialogue going if you haven’t already or to restart that dialogue with your revenue cycle team.”

With a new implementation date in place, now is the time for organizations to get back on track, and the best way to do that may be to opt into end-to-end testing, Coplan-Gould says. “I think it’s a good time to pick up the ball,” she says. Few other testing methods may be as valuable and affordable as end-to-end testing with payers. With the right level of preparedness, organizations may even be able to go through the process without the help of outside consultants, allowing them to allocate their valuable ICD-10 implementation dollars elsewhere, Coplan-Gould adds.
HIPAA demystified: Five myths and realities

Although numerous privacy and security laws apply to healthcare entities, HIPAA rules and requirements tend to receive the most emphasis—and generate the most angst. The terms HIPAA-compliant vendor, HIPAA cop, and HIPAA disciplinary action are anathema to experienced and serious privacy and information security professionals. HIPAA, as has been noted, represents the floor of requirements intended to protect the privacy and security of patient information. More stringent privacy requirements have existed at the state and national levels for several years before the HIPAA Privacy Rule was implemented (e.g., state medical records laws and requirements). Notably, many organizations implement policies and procedures that are more stringent than that required by HIPAA. Some of this is due to misinformation or misunderstanding of the HIPAA rules.

Greater focus on privacy and information security as key concepts embedded in patient care and organizational culture and a methodical approach to program development could make the process more logical and perhaps less onerous. Consider deleting the term HIPAA from policies and processes to the extent possible because this is not where an organization’s emphasis should lie.

Various myths and misconceptions surround HIPAA. Examples of HIPAA myth and reality include the following:

- **Myth: Security is an IT function.** Security involves safeguarding electronic information in various ways and by various means, including policies, processes, education, designation of security officers and managers, dedicating staff and monetary resources to providing technical tools, and physical safeguards to protect systems. The Security Rule includes only two standards related to technical security—access controls and audit controls. Most Security Rule standards address administrative safeguards. The rule also includes several physical safeguard and documentation requirements.

- **Myth: HIPAA is about enforcement, fines, investigations, and finding breaches.** HIPAA enforcement has been increasing since 2009 when OCR was empowered to oversee enforcement of the Privacy and Security Rules in 2003 and 2009, respectively. OCR also provides guidance, educational materials, and technical assistance in developing effective privacy and security programs. Much attention, including media coverage, has focused on investigations and enforcement actions. This, however, should not distract organizations from the true purposes of creating effective programs, providing...
patients access to their information, and developing health information exchanges to improve quality of care, care coordination, and patient engagement.

Effective training increases awareness of the real purpose of privacy and information security programs. Much of the negativity associated with HIPAA is dispelled when privacy and information security are key components of an organization’s culture. Privacy and information security and privacy officers must be empowered to do their jobs and must have resources to develop effective programs. Managers must undergo training to ensure they understand their important roles and responsibilities with respect to privacy and information security program effectiveness. This includes setting workforce expectations. Managers and workforce members are expected to meet organizational safety and quality goals, such as through personnel evaluations and performance improvement plans. Privacy and information security should also be included.

- **Myth: Focusing on limiting the use of devices that include ePHI and establishing restrictive policies will lead to fewer breaches and possible harm to patient information.** Security is not about restriction and limitation. Instead of erecting barriers to the use of technology, the emphasis should be on employing proven technologies (e.g., secure mobile technology, secure messaging) to ensure that patient care functions can be completed in a timely, safe manner.

Addressing security when planning and designing systems will eliminate the need for restrictive policies, and will remove the need for retrofits and additions after system implementation. Hard-wiring security into the system development life cycle and related processes will ensure that safe practices are followed.

- **Myth: HIPAA compliance is expensive and diverts resources from other important functions.** A majority (51%) of Ponemon survey respondents think HIPAA security and privacy regulations make delivering quality care more difficult. Most respondents (85%) said HIPAA reduces time available for patient care because of compliance tasks. However, those compliance tasks were not identified, and there is no direct correlation between the regulations and reduction in available time. Thus, this response is likely due to a lack of information and awareness of how security can enhance, not compromise, time spent with patients. Further, 79% of respondents claimed regulations complicate access to electronic information. This is simply not true. Secure biometrics, single sign-on technology, and proximity badges, when implemented properly, do not make access to electronic information more difficult. Consider, though, that many organizations still employ user logins and passwords and have many disparate systems that require separate and repeated logins due to system timeouts. These setups are onerous, but security itself is not the cause—the patchwork and outdated approach to it is. Privacy and security regulations should never hamper access to information necessary for patient care. Building in security at the start along with updating and improving systems should help this perception fade.

The goals of the meaningful use incentive programs, authorized by the HITECH Act, include promoting the use of EHRs, with the ability to share patient information on a national basis as the ultimate goal. Many providers that have received funding from federal and state meaningful use programs have attested that they have completed security risk analyses and remediated as appropriate. However, it is unclear whether they included privacy and security provisions in their system planning and implementation efforts. Failure to include privacy and information security officers in these decisions and not requiring vendors to provide adequate security without affecting system timeliness and effectiveness has led many organizations to develop work-arounds after implementation or to ignore many security provisions. This adds to system cost and delays acceptance and implementation of new workflows and processes.

Healthcare technology vendors must be required to build in security from the beginning and be transparent when working with healthcare providers. Security solutions should be adopted as part of systems development and testing processes, as is common practice in software companies, engineering firms, and other businesses involved in building security into new products and services.

**EDITOR’S NOTE**

Management matters

Social networking can help find ideal candidates

With so much information available online, it has become common for professionals to use social media to network and conduct job searches.

While job boards may be the most obvious place to post an open position or upload your resume, some employers and candidates look to social media when planning their next move. Similarly, sites such as LinkedIn, Twitter, and Facebook may provide HIM directors and managers with the tools and connections they need to work alongside human resources professionals to fill open positions.

“We are seeing more HIM professionals on LinkedIn and Twitter,” says Kayce Dover, president of HIM Connections, LLC, in Birmingham, Alabama. “Social media is a big part in our recruitment and networking process.”

An organization’s human resources professionals should be using social media, but they may not have the same professional connections as an HIM director or manager. “Human resources professionals who work in a hospital setting are often recruiting for a variety of departments and level of positions,” Dover says. “This makes it challenging for those recruiters to foster relationships with passive candidates in specialized areas.”

For this reason, HIM professionals should get to know people outside their organization and learn about the skills and expertise others in the industry possess, she says. Networking may put you in touch with a person who is an ideal candidate for the next opening in your department—and may even open doors to new opportunities for your career.

“When hiring for a position, you don’t want to limit yourself to only candidates who have submitted a resume online,” Dover says. “You want to cast your net as wide as possible to ensure you are hiring the best person for the job.” Leveraging the capabilities of social media can benefit organizations in various ways if used correctly. In addition to being a networking and recruiting tool, social media is often a form of marketing and requires a thoughtful strategy. Kayce Dover, president of HIM Connections, LLC, in Birmingham, Alabama, and Pat Lozito, chief operating officer of HIM Connections, recommend that organizations ask the following questions before encouraging workforce members to use social media for professional reasons:

- Is social media right for your organization?
- Who is your target audience?
- What are your objectives in using social media?
- How will your presence on social media help you accomplish your goals?
- Which social media platforms should you use (e.g., blogs, LinkedIn, Twitter, Facebook, Pinterest, YouTube)?
- How will you track growth and measure success?

Establishing a presence on social media websites is especially important for organizations looking to appeal to the younger generation who visit these pages frequently. “We’re dealing with a younger generation who are very technologically savvy,” says Pat Lozito, chief operating officer of HIM Connections. “They spend most of their life online, and the place to find them is Twitter, Facebook, LinkedIn—you have to appeal to that generation or you will lose them.”

Help your organization stand out

Dover has observed that today’s HIM job market is candidate-driven, which can present a challenge for HIM directors and managers who are looking to recruit qualified candidates. “Thinking outside the box and using creative recruitment methods will become even more important as we get ready to transition to ICD-10,” she says.
Sample social media policy

Establishing social media networking guidelines may help workforce members understand how to use social media websites to recruit candidates for open positions. However, organizations should also establish an overall social media usage policy. Refer to the sample below when your organization drafts or updates its social media policy.

At FACILITY NAME, we understand that social media can be a fun and rewarding way to share your life and opinions with family, friends, and coworkers around the world. However, use of social media also presents certain risks and carries with it certain responsibilities. To assist you in making responsible decisions about your use of social media, we have established these guidelines for appropriate use of social media. This policy applies to all associates who work for FACILITY NAME.

In the rapidly expanding world of electronic communication, social media can mean many things. Social media includes all means of communicating or posting information or content of any sort on the Internet, including to your own or someone else’s Web log or blog, journal or diary, personal website, social networking or affinity website, Web bulletin board, or a chat room, whether or not associated or affiliated with FACILITY NAME, as well as any other form of electronic communication. The same principles and guidelines found in FACILITY NAME policies and three basic beliefs apply to your activities online. Ultimately, you are solely responsible for what you post on the Internet. Before creating online content, consider some of the risks and rewards that are involved. Subject to applicable law, any online conduct that adversely affects your job performance, the performance of fellow associates, or otherwise adversely affects members, customers, suppliers, people who work on behalf of FACILITY NAME, or FACILITY NAME legitimate business interests may result in disciplinary action up to and including termination.

Know and follow the rules

Carefully read these guidelines and the FACILITY NAME Employment Handbook to ensure your postings are consistent with these policies. Inappropriate postings that may include discriminatory remarks, harassment, and threats of violence or similar inappropriate or unlawful conduct will not be tolerated and may subject you to disciplinary action up to and including termination.

Be respectful

Always be fair and courteous to fellow associates, customers, members, suppliers, or people who work on behalf of FACILITY NAME. Also, keep in mind that you are more likely to resolve work-related complaints by speaking directly with your coworkers or by utilizing our Open Communication Policy than by posting complaints to a social media outlet. Nevertheless, if you decide to post complaints or criticism, avoid using statements, photographs, video, or audio that reasonably could be viewed as malicious, obscene, threatening, or intimidating; that disparage customers, members, associates, or suppliers; or that might constitute harassment or bullying. Examples of such conduct might include offensive posts meant to intentionally harm someone’s reputation or posts that could contribute to a hostile work environment on the basis of race, sex, disability, religion, or any other status protected by law or company policy.
Sample social media policy (cont.)

Be honest and accurate
Make sure you are always honest and accurate when posting information or news, and if you make a mistake, correct it quickly. Be open about any previous posts you have altered. Remember that the Internet archives almost everything; therefore, even deleted postings are searchable. Never post any information or rumors that you know to be false about FACILITY NAME, fellow associates, members, customers, suppliers, people working on behalf of FACILITY NAME, or competitors.

Post only appropriate and respectful content
Maintain the confidentiality of FACILITY NAME trade secrets and private or confidential information. Trade secrets may include information regarding the development of systems, processes, products, know-how, and technology. Do not post internal reports, policies, procedures, or other internal business-related confidential communications. If you have questions about what is considered confidential, please check with the human resources department and/or your manager.

Respect financial disclosure laws
Company financial information is confidential and should never be posted or mentioned. Do not create a link from your blog, website, or other social networking site to the FACILITY NAME website without identifying yourself as a FACILITY NAME associate.

Express only your personal opinions
Never represent yourself as a spokesperson for FACILITY NAME. If FACILITY NAME is a subject of the content you are creating, be clear and open about the fact that you are an associate and make it clear that your views do not represent those of FACILITY NAME, fellow associates, members, customers, suppliers, or people working on behalf of FACILITY NAME. If you do publish a blog or post online related to the work you do or subjects associated with FACILITY NAME, make it clear that you are not speaking on behalf of FACILITY NAME. It is best to include a disclaimer such as "The postings on this site are my own and do not necessarily reflect the views of FACILITY NAME."

Using social media at work
Refrain from using social media while on work time or on equipment we provide, unless it is work-related as authorized by your manager or consistent with the FACILITY NAME Employment Handbook. Do not use FACILITY NAME email addresses to register on social networks, blogs, or other online tools utilized for personal use.

Retaliation is prohibited
FACILITY NAME prohibits taking negative action against any associate for reporting a possible deviation from this policy or for cooperating in an investigation. Any associate who retaliates against another associate for reporting a possible deviation from this policy or for cooperating in an investigation will be subject to disciplinary action, up to and including termination.

Media contact
Associates should not speak to the media on FACILITY NAME’s behalf without authorization from the CEO. All media inquiries should be directed to your manager.

Please contact your manager if you have questions or need further guidance.

Source: Reprinted with permission from HIM Connections, LLC, in Birmingham, Alabama.
When the October 1, 2014, ICD-10 implementation date was still in effect, Lozito noticed that some healthcare professionals—particularly coders, coding managers, and coding quality auditors—were on the lookout for new positions. “Candidates wanted to make a move prior to the transition, so we began to see a huge swapping of talent,” he says. “Many hospitals are already facing a staffing challenge, so this can create an even bigger recruitment challenge for HIM directors and managers.”

Consider the following to promote your organization and its open positions on social media websites:

- **Make connections.** Social media can be a great way to attract a potential new hire’s attention, whether your organization is actively hiring or you’re simply looking to network in case an opportunity comes up later, Lozito says.

  Some professionals may be comfortable in their current position, but might be open to considering a new opportunity. Social media is a way to engage potential candidates and inform them about opportunities at your organization, Dover says. Let people know that your organization may be the right fit when they make their next move. Ask your human resources professionals about the appropriate procedure for recommending a candidate and passing along information about the position, she adds.

  Make an effort to engage and connect with people online that hold positions similar to your own or to others in your department, Dover says. When a position opens up, your ideal candidate may be someone in your social media network. Recommending this person for a position as soon as it opens up may speed up the hiring process and prove beneficial for your organization overall, she adds.

  Connecting with a high volume of people is not as important as making quality connections. These relationships must be meaningful, otherwise you may not benefit from them. “Try to build a relationship and engage with your network,” Dover says.

- **Promote your organization’s culture.** Aside from searching for a candidate that meets the requirements for a given position, look for someone who will also fit in with your organization’s culture and contribute positively to the team, Dover says. “This can be just as important as the years’ experience a candidate might have,” she says.

  Go beyond developing a procedure for posting jobs on your website that lists the essential qualifications for candidacy. Let others know about your organization’s culture and share information that will entice people to apply for open positions, Lozito says. “This is how the new generation is going to be researching potential employers,” he says. “Social media is the way these candidates search for jobs.” In fact, he predicts organizations will increasingly turn to Skype and online technology to facilitate job interviews and offers.

  Share fun and interesting details about your organization’s culture with followers in your professional networks just as you would share details about a great new restaurant you tried or a fantastic movie you just watched with your friends. If something great is happening at your organization, inform everyone about it, Lozito says. “If we know of something good, we’re going to tell people about it,” he says. “You’ve got to leverage your networks.” Let everyone know about the fun you had at the annual company picnic or impromptu company ice cream social to keep things fresh and fun. When appropriate, share details about promotions, new hires, and employees who earned new degrees or certifications, Lozito says. “All of those things create a great presence for a company,” he adds.

- **Share job posts.** Once you have worked with human resources to develop a job description for an open position, ask how and where you can help promote it on social media. Your organization likely has policies in place that dictate appropriate social media guidelines, and these must be followed accordingly when networking in the general sense or posting job opportunities.

  Ask your organization’s human resources department how they plan to use social media to promote an open position and then find out how you can help. Organizations are typically open to the idea of allowing employees to share a link to a job board or a complete job description on social media, Dover says.

  “That’s going to be company policy just like any other company directives,” Lozito says.

  Posting about job opportunities online can be tricky. Find a way to ensure that the post captures the attention of your connections, but mix it up every so often so people don’t think your only motive for networking is filling a vacant position, he says. “You need to have a plan about how you are going to tackle social media,” Lozito says.
• **Discuss industry information.** Engaging with peers on social media is not just about promoting your organization or spreading the word about job opportunities. A key to building meaningful connections is finding a common ground. Share stories about hot topics in the industry to keep the conversation fresh, Dover says. Let others know what conferences you are attending so you can meet in person or help spread the word about exciting events. This may also help others see you as a leader in your industry, she adds.

Be careful not to inundate your connections with useless or redundant information. This may lead people to ignore your posts or remove you from their network. “Useless information leads to a very noisy environment,” Lozito says. “If you’re blasting your social networks with a lot of useful information, they’re going to see value in that. If it is useless information, they’re going to tune you out and they’re not going to pay attention to what message you’re trying to get across even if it is a great job opportunity.” Develop a strategy so that your posts are well balanced and helpful.

**HIM involvement in the search**

HIM directors and managers should keep the lines of communication open with their recruiters and human resources professionals throughout the recruitment process. Suggest professional websites on which they may want to post a job description, Dover says. They should remain engaged so they are aware of how the search is progressing.

Follow-up is recommended from all angles. Recruiters and human resources professionals should do their part, but so too should HIM professionals who refer candidates to their organization, Dover says. Something as simple as an automated reply may work for the initial application or testing process, but a more personal note may be appropriate for someone with whom you are networking.

Above all, recruiting the right candidate for the next open position means you must foster an environment that the current workforce can embrace. In addition to being rewarding and fun, the ideal workplace should also be flexible and offer your workforce members room to grow, Dover says.

**HIPAA Q&A**

**Disclosure of PHI and confidentiality agreements**

*by Chris Simons, MS, RHIA*

**Q** If someone calls a facility to schedule an appointment for a patient, is it a violation of HIPAA to admit the patient receives care at the practice?

For example, the practice where I work often helps victims of domestic abuse. We received a call from a patient’s estranged spouse who asked to schedule an appointment for the patient when, in reality, he was trying to determine the whereabouts of his spouse so he could harm her. I realize this is a safety issue but wonder whether it is also a HIPAA issue.

**A** I don’t see why you would need to confirm with the caller whether someone is currently a patient to make a new appointment. It is permissible to let others make appointments for patients, but this is because they are giving you information as opposed to you sharing information with them, which could be a HIPAA concern. I would be especially cautious when your intuition tells you that the caller may have an ulterior motive or you work someplace that often helps victims of abuse, as in your scenario. At minimum, I would ensure the appointment is confirmed with the patient directly and not with anyone else. Similarly, if someone calls looking for a patient currently in your office, the correct response is, “Due to privacy rules I can’t share that information with you, but leave your name and number and if I see [patient name], I will let him/her know that you are trying to get in touch.” Follow through with relaying the message to the patient if he or she is available. This patient-friendly approach should protect your patients’ privacy.
**Q** A former employee at the agency where I work disclosed one patient’s information to another patient while still employed by the company. The confidentiality agreement each employee signs states that patient information will remain confidential during and subsequent to employment. Is the agency required to treat this as a breach? Can the agency sanction the former employee?

**A** The HIPAA Omnibus Rule requires every potential incident to have a documented risk assessment. In this case, you don’t indicate whether the disclosure was deliberate or accidental, or the nature of the information disclosed. It certainly sounds like notification would be required if PHI was disclosed to another patient, assuming the recipient was able to retain the information. As to sanctions, the employee left the organization, so there isn’t much you can do apart from not giving him or her a good reference or reporting the former employee to his or her professional board, which could be considered if applicable. (Consult legal counsel before taking that step.) The employee could be held civilly or criminally liable should the patient whose information was breached choose to file an OCR complaint and OCR were to find that the breach was worthy of pursuing to that level (unlikely but possible). Remember, your records of training and auditing are important to show that you have done your best to protect your patients from inappropriate access to PHI.

**Q** While at an appointment, I noticed a staff member place patient folders in a stand on top of the counter at the registration desk, easily accessible to anyone nearby. I noticed a receipt sticking out of one folder, and I could read the patient’s name, last four digits of his or her Social Security number, and diagnosis/billing codes. Is this a HIPAA violation, since anyone walking by could read this information, or is it just a bad practice?

**A** HIPAA requires that covered entities minimize and mitigate incidental disclosures such as the one you describe. The practice should not leave documents where those who are not authorized to access them could do so and should not speak of details where unauthorized persons may overhear. The practice would be required, based on a complaint you might voice, to do a risk assessment of the incident to determine if it is an actual breach. The key to that assessment would be determining whether you could have reasonably retained the information you saw. That you could view the patient’s Social Security number is concerning. Depending on where the organization is located, you may also have to comply with state-specific notification requirements. Bottom line: It is definitely a poor practice and quite possibly a breach that would require notification to HHS and to the patient whose information you saw. I would recommend you report it to the organization so they can rectify this potential problem.

**Q** Within our pharmacy dispensing system, we have the ability to enter free form notes for certain records such as a patient record, prescription records, and physician records. The notes entered in the patient record are customer-service focused and not treatment- or payment-related in nature. Would these notes be considered PHI, and would there be a retention requirement concerning these notes prior to purging the patient notes?

**A** Anything documented is potentially discoverable. The information in your system is undoubtedly PHI as it certainly contains patients’ names, dates of birth, and other demographic information. Remember, for the notes to not be considered PHI, they must be stripped of all 18 elements that constitute PHI. For additional guidance on this, visit [www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html](http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html).

I recommend consulting your attorney or risk management company for guidance on this question, as retention laws vary from state to state. You should definitely have a written policy that specifies exactly what constitutes your legal health record (LHR), since presumably there are many pieces of information in your organization (e.g., in your pharmacy system) that you do not routinely consider part of your LHR. Also, consider whether this information is maintained elsewhere and, if so, whether it could be destroyed under the theory that it could be reproduced from the alternate location if needed.

**EDITOR’S NOTE**

Simons is the director of health information and privacy officer at Cheshire Medical Center/Dartmouth-Hitchcock in Keene, New Hampshire. Simons is also an MRB advisory board member. This information does not constitute legal advice. Consult legal counsel for answers to specific privacy and security questions. Send your questions related to HIPAA compliance to Editor Jaclyn Fitzgerald at jfitzgerald@hcpro.com.
A Minute for the Medical Staff

Telling the whole story: CliffsNotes™ don’t work in medicine

Along with being knowledgeable about their patients, physicians must ensure patients’ medical records tell the whole story about the conditions they’re treating and that the records reflect all known information. This is critical not only for meeting the needs of the patients in their care, but also for meeting the needs of the patients while they are under someone else’s care. If a physician goes on vacation, retires, gets in an auto accident, or takes a trip to Mars, someone else has to know the patient’s story. In addition, with the changes to reimbursement, the less story a physician reveals, the less the resulting bills may be worth. The traditional way of selecting professional E/M codes may not last much longer. Other methods have been utilized extensively, including Hierarchical Condition Categories and severity-adjusted payments based on complexity of ICD-9 codes.

For example, I was recently at the hospital for a procedure. The specialist I saw examined me, ran tests, came up with an idea of what was needed to be done, and scheduled me for the procedure. When I was leaving the office after scheduling the procedure, I viewed the superbill the physician would submit to my insurer. He had put a check mark next to the ICD-9-CM code for my symptoms, but did not check off a code for the disease that was the reason for the operation. As a result, the physician would certainly be paid for the visit, but I would have been turned down for the procedure because of the lack of documentation validating what he planned to do. The physician wouldn’t have been paid for the procedure either if he performed it without knowing about the denial. A whole bunch of diseases could have caused my symptoms, only one of which was the one the physician planned to address with the procedure. The ICD-9 codes didn’t tell the whole story.

Many people are diagnosed with diabetes. They visit clinics in the community, private practices, and major medical centers. Treating diabetic patients can be simple or complex. If the codes an organization turns in don’t tell the full story of the patient’s symptoms and the complexity of the case, the visit will be paid out at the lowest value for the basic form of the disease.

Many of these providers have a routine. They see Type 1 (ICD-9-CM code 250.02) or Type 2 (ICD-9-CM code 250.00) diabetic patients, so those may be the only ICD-9-CM diabetes codes on their superbills. There may be no options on some superbills for the physicians to check off uncontrolled diabetes, diabetes caused by other processes, or any of the manifestations of diabetes at all. In fact, I saw a superbill from one office where the only diabetes code was 250—and that code doesn’t exist.

Physicians should make time to talk to their office folks about the complexity of the diabetic patients they treat. Physicians should ensure their superbill includes a variety of codes so they can bill for specific encounters such as the neurologic manifestation of gastroparesis, which the physician is treating with dietary control and consideration of a percutaneous endoscopic gastrostomy tube. Don’t forget about codes for the patient with Stage 3 chronic kidney disease (CKD) due to diabetic nephropathy or the patient with anemia of Stage 3 CKD that just started on erythropoietin. Through documentation, physicians can ensure they can code for the patient with proliferative retinopathy whom they referred to an ophthalmologist for laser treatment. If physicians don’t consider coding and billing for complex cases, they’ll have a record of only treating healthy
A Minute for the Medical Staff is an exclusive service for subscribers to Medical Records Briefing.

Reproduction of A Minute for the Medical Staff within the subscriber’s institution is encouraged.

Reproduction in any form outside the subscriber’s institution is forbidden without prior written permission.

Robert S. Gold, MD