SUMMER 2010

CORRIDORS

News for North Carolina Hospitals
from the Health Law Attorneys of Poyner Spruill LLP

Audits and Breaches and Fines, Oh My! It's time to make sure your HIPAA privacy and security compliance program has you covered

by Elizabeth Johnson

If you don't feel confident about your organization's HIPAA privacy and security compliance, now is a good time to undertake a refresher. Here are a few reasons why (followed by a discussion of what you can do to improve your program).

Meaningful use incentives. As part of its proposed rule to implement "meaningful use" incentives, the Centers for Medicare & Medicaid Services (CMS) dictated that eligible professionals and hospitals must "[c]onduct or review a security risk analysis . . . and implement security updates as necessary." If you comply with the HIPAA Security Rule, you will have met this Stage 1 requirement for "meaningful use."

Breach notification. You probably know by now that your organization is obligated to report breaches of protected health information (PHI) to both affected individuals and Health and Human Services (HHS) (and, in some cases, the media). Existing breach notification laws at the state level have taught us that sending the requisite notifications often prompts a government investigation of privacy and security compliance and sometimes spawns lawsuits by affected individuals. Ensuring compliance prior to one of these events can mitigate its impact, in part by minimizing the risk of a government enforcement action and as a defense to a potential lawsuit.

Government Enforcement. For several years, regulators have been taking enforcement actions against organizations that report security breaches. In the typical pattern, the regulators investigate, find the incident demonstrating inadequate security, and charge the organization with an unfair trade practice pursuant to federal or state law. A case in point was the HHS-FTC joint enforcement action against CVS Pharmacy. The result was a settlement with both agencies, including a $2.25 million payment by CVS and an agreement to implement a comprehensive, written information security program with oversight from HHS, as well as to submit to audits of compliance with that plan biennially for 20 years.

Increased penalties. The HITECH Act was full of motivators to compel HIPAA privacy and security compliance. The same statute that brought you breach notification and additional privacy and security obligations also increased the penalty amounts HHS can seek for noncompliance. Whereas penalties were previously capped at $25,000 for multiple violations of the same provision in a single calendar year, they are now capped at $1.5 million.

Mandatory audits and state enforcement. In case breach notification and increased penalty amounts were insufficient compliance incentive, the HITECH Act also made periodic HIPAA audits by HHS mandatory and authorized state attorneys general to enforce HIPAA. The Connecticut attorney general has already brought such an action, and Office for Civil Rights (OCR) has indicated that it intends to audit every covered entity that reports a breach affecting more than 500 people.

continued on page three

NEW HEALTH CARE DECISIONS POSTER IN THIS EDITION – At the request of one of our readers, we developed this poster for use in health care facilities in North Carolina. Please unfold and enjoy.

p.s. Poyner Spruill LLP
ATTORNEYS AT LAW

RALEIGH CHARLOTTE ROCKY MOUNT SOUTHERN PINES WWW.POYNERSPRUILL.COM

301 Fayetteville St., Suite 1900, Raleigh, NC 27601/P.O. Box 1801, Raleigh, NC 27602-1801 P: 919.783.6400 F: 919.783.1075

Tips for Successful Medical Staff Hearings

by Steve Shaber

Few events are more distasteful to both hospitals and medical staff leaders than hotly contested medical staff hearings. They often challenge medical staff's goal of fostering collegiality and hospitals' cultivation of trust and good relations with their physicians. Let's begin with three observations.

- Everyone hates medical staff fair hearings.
- When it comes to fair hearings, actions the medical executive committee (MEC) takes that adversely affect the hearing almost always happen before the hearing begins.
- Physicians often come out better at a hearing than the MEC had recommended; hearing panels often disagree, at least in part, with the MEC's desired corrective action.

If the third observation is true, then many hearings should have been avoided. If the second observation is true, then many hearings where the physician wins could have been avoided. Finally, if the first observation is true – and it surely is – whenever a hearing can be avoided, everyone will be happier.

We hope that this article will facilitate the happiness of all parties by helping them to avoid unnecessary hearings.

What is the first thing to remember? Staff fair hearings are rare. Even the state's largest hospitals go years between one hearing and another. Small hospitals may go a couple of decades without a hearing. This means that typically no one at a hospital is particularly expert when it comes to preparing for and running a hearing, and many people are novices. Of all the parties to the hearing, the medical staff's rotating physician leadership is most likely to be inexperienced.

There is an easy remedy for inexperience: think ahead and prepare accordingly. Assume the matter will go to a fair hearing, and plan from the start for that eventuality.

Gather the whole story. Most staff hearings take the form of an appeal from the medical executive committee's decision to take adverse action against a physician. Most staff bylaws say the MEC decision is presumptively correct, and the burden is on the physician to prove the MEC had no reasonable basis for its decision.

Hearing panels dislike this presumption against the physician, and they will find a way around it unless they are convinced the MEC actually heard all the evidence about the case. On at least one level, this attitude makes sense. Why would a hearing panel of physicians defer to the MEC, when the panel believes it knows more about the case than the MEC did?

The solution is to be sure the MEC has gathered the whole story before it takes corrective action. Gathering the whole story means talking to everyone who is involved – not only those who do not support the physician, but those who support him or her. It means knowing whether potential witnesses are willing to testify under oath at a hearing. It means documenting what everyone says in enough detail so the MEC gets the story in the words of the witnesses, not just in the words of the investigators.

Beware of bias. The people complaining about the physician may have a bias that needs to be recognized and considered in evaluating their credibility, well before the MEC takes corrective action and the case heads toward a hearing. Complaints come from many sources, and every complainant may have several motives: partners fall out; specialists and primary care physicians quarrel; nurses and physicians clash; competing specialists vie for business; and administrators and departments look out for their staffs and their own. The MEC should identify these problems and take them into account from the beginning, because the hearing panel certainly will learn about them if the case ever comes to a hearing.

Talk to the doctor. It is impossible to gather the whole story without hearing from the physician who is the subject of the investigation, in person and in detail. Yet the MEC often does not make this contact, and, instead, either relies on the physician's written statement or on what it perceives as the "incontrovertible facts of the case." The problem with only receiving the physician's account in writing is that it leaves unanswered questions the MEC may have – and there are always questions. The problem with relying on the so-called "incontrovertible" facts is they often do not tell the MEC what it needs to know about the physician's attitude. Two physicians may make the same serious error, but each may deserve different corrective action if each has a different attitude toward the events. One physician may have learned from the situation and may be trusted to avoid such problems in the future. The other may have learned nothing and cannot be trusted. The best way to judge the physician's attitude is to talk face-to-face.

Be sure there is a connection to good medicine. The federal Health Care Quality Improvement Act protects everyone involved in a staff fair hearing from personal liability if they act in the good-faith belief that their actions promote quality health care. Consequently, it is important to ask from the beginning to the end of this process, have the physician's actions impinged on good health care, and does the proposed corrective action promote it? Do not start on a course that may lead to a hearing unless you can say the physician's actions either have, or most likely would, seriously interfere with good health care at the hospital. The hearing panel will certainly ask this question.

Step back and be sure of your case. The MEC probably should not take action that will lead to a hearing unless it is confident it will win. A good way to test that confidence is to ask whether the medical staff would win the hearing (and the physician lose), even if the burden were on the staff to prove that all the events occurred, there were no extenuating circumstances, and the proposed corrective action is precisely warranted by the errors committed. This is not to say that from a legal perspective, the burden is on the medical staff. Rather, the MEC's acting as if the burden were always on the staff builds in an extra layer of assurance that the hearing panel will see things the same way.

Conclusion. These suggestions come to a single point. If the MEC puts itself in the shoes of the hearing panel and is doubly careful before it starts any sort of corrective action that could lead to a hearing, it will be less likely to start such serious corrective action. Moreover, if and when the MEC starts such corrective action, it will be better able to prove to a hearing panel that the corrective action was needed. As a way to avoid unnecessary hearings, we believe that this is the road to happiness.

For more information on medical staff hearings or other health law-related issues, please contact **Steve Shaber** at **919.783.2906** or **sshaber@poynerspruill.com**.

Audits and Breaches...
continued from page one

Threats to Medicaid and Medicare reimbursement. In case you were thinking that the worst-case scenario in a breach situation would be allegations of HIPAA violations and a potential fine, consider the case of Wentworth-Douglass Hospital in Dover, New Hampshire. That facility has been the subject of an investigation by the New Hampshire attorney general following an alleged breach of patient medical records. What's different about this investigation is that CMS joined the investigation, sending surveyors from the New Hampshire Department of Health and Human Services to examine not only privacy and security issues, but also patients' rights and quality assurance in order to determine whether the facility meets the "conditions of participation" for reimbursement by Medicaid and Medicare.

What to Do? Further Progress along the HIPAA Brick Road

With all these compelling reasons to revisit your HIPAA privacy and security compliance, you may be wondering where to start. Some suggestions:

Know your obligations. Your first step is to identify all legal requirements governing your organization. For privacy and security purposes, these are enumerated in the HIPAA Privacy, Security, and Breach Notification Rules. You need to identify each requirement that should lead to some "end product" or response by your organization. Depending on the requirement, that could mean a documented policy or procedure, a set of security reminders, training programs, a complaint process, an incident response plan, etc. If you've never asked a lawyer to review your program to determine whether each of these end products is addressed, this might be a good time to consider that step.

Identify and address gaps. Once you have identified all of the requirements that require an end product, it's time to review your program to see if it actually consists of all those pieces. Is anything missing? Where are your gaps? Once you have found the gaps, they need to be addressed, which may mean drafting a policy, conducting training, instituting a new procedure, or preparing some other "end product," depending on the requirement you are trying to address.

Test your program and consider lessons learned. Assuming you have all the pieces in place, it's time to consider how well they actually work. If you have a complaint process in place as is required, how effective is it? Has it ever been used? If not, should you test it to determine how well it would work? The same questions can be asked of your security incident response plan, your procedure to address individuals' requests for access and amendment of their information, your

continued on page five

Risk Analysis – a Critical Step One in Safeguarding e-PHI

by Pam Scott

For hospitals and other health care providers working to secure electronic protected health information (e-PHI), a comprehensive risk analysis is a critical first step. The draft guidance on risk analysis issued on May 7, 2010, by the Department of Health and Human Services' Office for Civil Rights (OCR) offers a starting point to help hospitals and other providers identify and implement the most effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI. The guidance, which is available online at www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/radraftguidanceintro.html, provides helpful insight into the expectations of OCR, the agency responsible for enforcing the HIPAA Privacy and Security Rules.

The HIPAA Security Rule has always required health care providers, health plans, and other covered entities to conduct an accurate and thorough analysis of potential risks to the confidentiality, integrity, and availability of e-PHI, but it does not specify how to go about conducting an effective assessment. The risk analysis requirement has received heightened attention recently in the wake of stronger enforcement provisions included in the HITECH Act for violations of the HIPAA Privacy and Security Rules, as well as the inclusion of this security measure in the "meaningful use" rules under which eligible health care providers can qualify for the electronic health record incentives program adopted last year.

OCR's draft guidance recommends that organizations include the following key steps in their risk analysis.

- Define the scope of the risk analysis.
- Identify where e-PHI is stored, received, maintained, or transmitted.
- Identify and document reasonably anticipated threats and vulnerabilities that could lead to improper disclosure and access.
- Evaluate current security measures to safeguard e-PHI.
- Determine the likelihood and impact of potential risks to the confidentiality, integrity, and availability of e-PHI.
- Determine the level of risk for reasonably anticipated threats and vulnerabilities identified during the analysis.
- Document the risk analysis.
- Periodically review and update the risk analysis.

OCR's guidance indicates that the risk analysis process should be an ongoing process in order to identify new threats to the confidentiality, integrity, and availability of e-PHI and to identify and implement necessary updates, as required by the Security Rule. The guidance recognizes that the frequency of the risk analysis will vary according to the specific needs and circumstances of each organization. It also wisely notes the value of incorporating risk analysis in planning on the front end for an organization's new technologies and operations. OCR's reported plan to conduct compliance reviews for all HIPAA data breaches involving data for more than 500 individuals highlights the importance of implementing a continuing, comprehensive risk analysis.

For more information on e-PHI or other health law-related issues, please contact **Pam Scott** at **919.783.2954** or **pscott@poynerspruill.com**.

Mind Your PHI – Even in the Trash

A Greensboro urgent care center recently agreed to pay $50,000 to settle a case filed by the N.C. attorney general after the center's discarded patient records for more than 750 individuals were discovered in a Dumpster, complete with individuals' names, Social Security numbers, birth dates, insurance account numbers and PHI. The center had hired a contractor to destroy the records. The attorney general brought the action under the State's Identity Theft Protection Act. The act requires businesses to adopt formal policies and procedures for secure disposal of records containing personal information and to take steps to ensure that any contractor hired to destroy such records is reputable and competent. This case highlights the value of investing time and resources in secure record destruction and due diligence of record disposal contractors, which would likely cost much less than the monetary penalties a health care provider faces for illegal dumping of patient records.

Audits and Breaches...
CONTINUED FROM PAGE THREE

contingency or emergency mode operation plans, and other required aspects of the HIPAA rules. Your actual experiences using these procedures should inform your updates to them – what worked, and what did not? If you haven't had an actual situation requiring you to put the procedures into practice, reconsider them in light of operational changes and consider a "tabletop" test – a test run to determine whether and how they would work. If it comes up short, it's time for some modifications to the approach.

Security Rule compliance. Security Rule compliance deserves some special consideration. Whereas Privacy Rule compliance is primarily administrative, such as implementation of policies and procedures, Security Rule compliance is one part administrative safeguards and two parts physical and technical safeguards. That means that covered entities have to take a multidisciplinary approach to compliance. When we assist clients in a Security Rule compliance review, we always ask to meet with their IT personnel or provider. You simply cannot assess compliance with this rule unless you ensure that the physical and technical security controls are in place. More than likely, you will have to explain the legal obligations to your IT staff and, through a series of discussions with them, determine whether their existing security measures, policies, and procedures meet the rule's requirements. Very often, an existing security measure is appropriate but has not been documented. In such cases, the requirements are not met, due to the lack of documentation.

Another important aspect of the Security Rule is dealing with "addressable" implementation specifications. Covered entities may have an option not to implement those specifications denoted as "addressable," but only after they complete and document an assessment to determine whether the specification was reasonable and appropriate for the organization in light of the size, complexity, and capabilities of the organization; the probability and criticality of the potential risks to information; the cost of implementation; and the organization's technical infrastructure. This process need not be daunting, and a legal review is often appropriate in order to complete the task.

Business associates. As a result of the HITECH Act, all your business associate agreements require an update. More important, you need to make sure that your business associates are complying fully with the Security Rule, another new obligation imposed by the HITECH Act. Previously, your business associates' security measures needed only to be "reasonable and appropriate," which is a far cry from complying fully with the more than 60 specific safeguards outlined in the Security Rule. If they aren't complying, your business associates are putting your protected health information at risk. That risk is now greatly exacerbated by the breach notice obligations, which require covered entities to provide notification letters when security incidents are caused by their business associates. In other words, your business associate's security lapse could result in substantial notification costs and enforcement risks for your organization. These costs and risks are further magnified by the increased HIPAA penalties, audits, and enforcement also implemented by the HITECH Act.

Paper the problem. When the Office of Inspector General audited Atlanta's Piedmont Hospital on Security Rule compliance in March 2007, it gave Piedmont 10 days to respond to a list of 42 questions and requests. To comply with a request like that, you want to have all your compliance paperwork pulled together in a single location, fully organized, and up to date in advance of receiving the inquiry. Once you determine that you have all the requisite pieces documented, you must get organized. At a minimum, that means collecting together all the following.

- All requisite HIPAA privacy policies and procedures
- All requisite HIPAA security policies, procedures, security plans, security reminders, documentation of access rights, etc.
- Requisite HITECH breach response procedures
- Notice of privacy practices
- Log of HIPAA training
- Accounting of disclosures for the past six years
- Hybrid entity designation (if applicable)
- Log of security incidents
- Your organization's business associate agreements

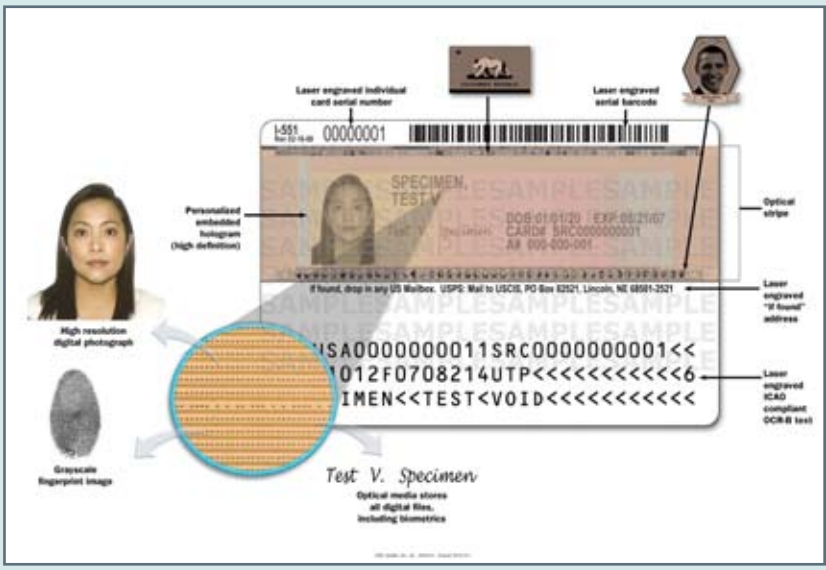
The new HITECH requirements have substantially increased the obligations of health care providers and their business associates, and the stakes are high. Now is an excellent time to review your HIPAA privacy and security compliance programs and their implementation.

Elizabeth Johnson's practice focuses on privacy, information security, and records management. She may be reached at 919.783.2971 or ejohnson@poynerspruill.com.

The Green Card Is Finally Green Again!

by Jennifer Parser

After May 11, 2010, employers being shown a strange new green card as part of the I-9 employment eligibility verification process should not assume the worst. The "permanent resident card" has been redesigned to be green in color and include biometrics in the form of a laser-engraved fingerprint, holographic images, and high-resolution microimages of all the U.S. presidents and state flags. There is also an embedded radio frequency identification device allowing Customs and Border Protection to read the card from a distance. A preprinted return address on the back enables return of lost cards to the U.S. Citizenship and Immigration Services (USCIS). Old green cards are acceptable but upon expiration will be renewed in this redesigned format. The USCIS is recommending that holders of green cards without an expiration date renew them to be in conformity with this format or consider becoming naturalized U.S. citizens. Overlaying the old green card in the graphic to the right* is a sample of the new green card with salient points highlighted. (To view these graphics on a full screen, visit http://www.poynerspruill.com/publications/Pages/GreenCardFinallyGreen.aspx and click on the cards.)



* Source: American Immigration Lawyers Association

In reviewing this type of documentation as part of the I-9 process, an employer is guaranteeing to Immigration and Customs Enforcement, not the legitimacy of the status of the person presenting the document, but rather the facts that (1) its HR manager has reviewed the original document, (2) the document reasonably appears to be genuine, and (3) the document relates to the employee who has presented it for employment eligibility verification purposes.

A reminder: a policy of copying and retaining the copies of documentation offered by an employee when completing the I-9 must be done uniformly for all employees. Also, the I-9s with any copied identity and employment authorization documents must be retained for at least three years from the date of hire or one year after termination of employment, whichever is longer.

The I-9s and any copied documentation (like this new green card) relating to the I-9 completion should be kept separate from all other employee information.

Jennifer Parser practices in the areas of immigration, employment, and international law. She is licensed in the state of New York and is not licensed in North Carolina. Jennifer may be reached at **jparser@poynerspruill.com** or **919.783.2955**. Elizabeth Johnson contributed to this article.