HIPAA Compliance: A Step-by-Step Guide Using the Structure of Your Compliance Program

Here is advice from Washington, D.C., attorney Michael Bell on integrating privacy and security requirements into your compliance program. Every week for the next few weeks, Bell will tackle different elements of effective compliance programs in terms of HIPAA. Contact Bell, who is with the law firm of Mintz, Levin, Cohn, Ferris, Glovsky and Popeo PC, at (202) 434-7481.

Now that the health care industry has come to grips with the fact that the privacy regulations are going into effect, provider consent forms are still required, and the "minimum necessary" standard is here to stay, organizations must grapple with the pressing question, *"Where do we start?"*

First, take a breath and relax. Most of you reading this publication already have endured the trials and tribulations of establishing a corporate compliance program. Start there. As illustrated below, an operational compliance program provides the perfect infrastructure within which to create a fully functional and compliant HIPAA privacy and security program.

7 Elements of a Corporate Compliance Program	HIPAA Security Requirements	HIPAA Privacy Requirements
Policies and Procedures	Administrative Procedures	Documentation of Policies and Procedures
Assignment of Oversight Responsibilities	Assigned Security & Privacy Responsibility	Designated Privacy Official
Training and Education	Training and Education	Training
Lines of Communication	Report Procedures; Event Reporting	Complaint Processing
Enforcement and Discipline	Sanctions	Sanctions
Auditing and Monitoring	Internal Audit	Accounting for Disclosures
Response and Corrective Action	Response Procedures; Testing & Revision	Duty to Mitigate

In addition to the infrastructure, health care organizations, through records management programs, departmental policies, and / or compliance programs, maintain policies and procedures and conduct training relating to the confidentiality of medical and other personal records. Therefore, start by understanding what already is in place by conducting an assessment and inventory of current practices. After identifying the origination, uses, disclosures, and final disposition of the protected health information, you will be able to establish organizational priorities, otherwise known as your work plan.

Part 1: The Assessment

The internal assessment will provide a snapshot of the organization's current compliance with the regulations that will serve as a blueprint for the development of the organization's HIPAA program. Ideally, an internal HIPAA assessment should, at a minimum, identify the following:

(1) Concise information flow within the organization. Using a tailored questionnaire / survey, develop both "macro" and "micro" information flow charts. At the macro level, trace the path of personal information throughout the organization. Identify the following elements: content of the information; the locations, including subsidiaries, sister companies and business associates; where the information is used and transferred within and outside the organization; the different uses for the information; and the final disposition of the data. At the micro or more granular level, trace the flow of information within each business unit and department. Again, identify the same elements, but at the unit or individual level.

With regard to security, create or update your organization's information system mapping (consider using schematics and other materials prepared for Y2K), specify all internal and external network access points. Identify security mechanisms employed (e.g., intrusion detection systems, firewalls and settings, client and server security in enterprise systems, cryptography, virus detection, etc.).

(2) The responsible parties. The survey should also produce a list of key players for the initiative. Not surprisingly, health care organizations are turning initially to corporate compliance people because they are most familiar with the process of implementing organization-wide programs. Although other members of the organization may eventually constitute the organization's privacy and security committees or sub-committees, the knowledgeable compliance staff (with the assistance of the Information Systems (IS) department) are best equipped to commence the process by creating, distributing and collecting questionnaire / assessments.

continued

(3) A compliance benchmark. In addition to producing a comprehensive flow chart and responsible parties, a well designed assessment survey will yield a snapshot of the organization's current compliance with the requirements of the regulations. Include in your organization's assessment a checklist comprised of the requirements set forth in the regulations. Through this simple, albeit time-consuming step, you should be able to identify areas and systems that will require the greatest needs by way of compliance.

(4) Risk analysis and prioritization. Although not specifically provided for in the regulations, prioritize the identified weaknesses pursuant to the types of information involved.

(5) The organization's long-term e-Health strategy. A consequence of these regulations, combined with greater access to affordable technology, has been unprecedented attention to eHealth initiatives. To this end, an important part of a HIPAA assessment is the identification of the organization's short- and long-term eHealth initiatives. Whether the strategic initiatives include on-line or wireless access to medical information or simply greater customer outreach, HIPAA and other laws and regulations such as The Children's Online Privacy Protection Act (COPPA) will likely impact the plan.

As you can see, there are many advantages to beginning your HIPAA initiative with a well-designed, comprehensive internal assessment that is tailored to your organization.

Next week: Part 2, The First Three Elements of a HIPAA Compliance Program: Policies and Procedures, Oversight Responsibility, and Training.

Employee Questionnaires Reveal Compliance Concerns, Lead to Policy Changes: Information Is Fed Back to VPs

Health Care Services Corp. might never have found out about some monkey business inside its own walls if it hadn't been for a little note written by an employee on the company's compliance questionnaire. The former employee responded to the 15 questions on the questionnaire (see p. 5) and then added a note reporting that another employee was using company assets to print documents for his wife's business.

After an investigation, compliance director Bob Frederick found that "most of the information provided by the former employee was accurate." HCSC responded with disciplinary action, including the loss of an annual salary increase, six months probation, additional compliance training, and a written corrective action plan.

The exit compliance questionnaire is one method used by the insurance company to solicit employee feedback and extract reports of potential misconduct, says Fred Verinder, vice president of compliance operations. The answers to the questions, along with other data, are compiled in a database, and the results are fed back to the vice presidents of every division in summary form. The VPs use the data to address concerns raised by current and former employees. "We are identifying issues through this process that were not coming to us in other ways," Verinder notes (for a compliance investigation protocol, see p. 6).

Questionnaires are sent by registered mail to all former employees. Verinder says HCSC anticipates a 26% response rate. When the completed questionnaires come in, Frederick reviews them and decides which require an investigation.

When the investigation is done, he enters the results in a database and looks for trends. If Frederick spots a particular problem that calls for more employee training, he coordinates with the managers of the relevant department.

Frederick assigns a percentage factor for each of the 15 questions that correlates an overall corporate response with the division response. This lets the vice

AIS HCFA/IG Library

Visit www.AISHealth.com/Compliance/HCFAIGLibrary.html, or merely click the "Compliance" channel on www.AISHealth.com, for these and other documents from HCFA and the HHS/IG:

- Medicare Enrollment Forms
- Final Stark Self-Referral Rule
- Summary of Key Stark Rule Points
- The Orange Book
- OIG Advisory Opinions
- HCFA Q&As on OPPS
- HCFA Program Memorandums
- OIG Work Plan for 2001
- Medicare Exclusions & Reinstatements
- OIG EMTALA Reports
- CIAs and Settlement Agreements

HIPAA Compliance: A Step-by-Step Guide, Part Two

In the April 19 Report on Medicare Compliance, *attorney Michael Bell explained how the requirements of the HIPAA regulations can be separated according to the seven elements of an effective corporate compliance program. Consequently, your compliance program is an excellent vehicle to launch the organization's HIPAA privacy and security program. In this week's installment in our series on integrating HIPAA privacy and security requirements into existing compliance programs, Bell briefly discusses the first element of a HIPAA compliance program: policies and procedures. Contact Bell, who is with the Washington, D.C., law firm of Mintz, Levin, Cohn, Ferris, Glovsky and Popeo PC, at (202) 434-7481.*

Part 2: The First Element of a HIPAA Compliance Program: Policies and Procedures

The privacy regulations provide that a "covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart." Likewise, the proposed security regulations require that covered entities maintain "documented, formal practices to manage the selection and execution of security measures to protect data, and to manage the conduct of personnel in relation to the protection of data."

Despite the similarities in these requirements, the policies themselves and their applicability to the workforce differ significantly.

Generally, an effective privacy / security policy and procedure should inform employees and contractors of their obligatory requirements for protecting patient-related and other personal or proprietary information. A policy and procedure should serve as an information resource that clearly defines and addresses the employees' most basic questions: who, what, where, when and how.

In addition, to facilitate periodic updates and revisions, each policy should contain cites to the legal or corporate authority that serves as the basis for the policy. Consider attaching copies or summaries of the applicable statutes and regulations or corporate policy as an addendum to the policy.

Adapt and Update Existing Policies

Many health care organizations can and should build on existing corporate compliance policies and procedures to address several of the privacy and security requirements. For example, both the privacy and security regulations mandate the designation of oversight personnel, employee training, discipline of employees who fail to abide by the privacy and security policies and procedures, incident reporting, and corrective action — all requirements of a corporate compliance program. Thus, because most health care organizations already maintain compliance program policies and procedures that address these very topics, the most efficient course of action would be to update and amend these policies and procedures to account for the requirements contained in the HIPAA privacy and security regulations.

With regard to privacy policies and procedures specifically, covered entities are required to develop both a Notice of Privacy Practices and specific policies and procedures that evidence compliance with the requirements. Drawing on the corporate compliance analogy, an organization's Notice of Privacy Practices is similar to a Code of Conduct in that it sets forth the basic tenets of the organization's privacy program. However, unlike a Code of Conduct, the format and content of the Notice of Privacy Practices is specified by regulation.

On the other hand, because each department within an organization obtains, uses and discloses different information for different purposes, the privacy policies and procedures should be tailored to the functions of each business unit and / or department (if applicable).

While policies and procedures will differ from department to department, there will be at least one common element among the policies: incorporation of the "minimum necessary" standard. Use the internal assessment, and specifically the information flow chart, to ascertain the types and content of information, all uses and disclosures, and the purposes of such uses and disclosures within each department. This information will allow for a concise, targeted departmental privacy P&P and informed decision-making with regard to the "minimum necessary" compliance requirement. Obviously policies and procedures for intake personnel, such as admission, registration and field representatives, would have to account for authorizations and consent if applicable. In contrast, clinicians and other departments in the organization will need policies and procedures that will primarily focus on appropriate use and disclosures within the department.

Unlike privacy policies and procedures, in health care organizations the majority of P&Ps drafted to

comply with the proposed HIPAA security standards will not have general application to the workforce. With the exception of the "chain of trust" agreement and certain other administrative and physical safeguard requirements, the proposed security standards are technical and systems-oriented.

Consequently, the vast majority of the security policies and procedures designed pursuant to these requirements will be applicable only to personnel responsible for information systems configuration, administration and maintenance (e.g., information technology / systems staff). Notwithstanding, these security policies and procedures are equally important as those drafted for privacy compliance.

Due to the security standard's technical nature and impact on operations, the organization should designate the following positions (or their equivalent) to create and review the security P&Ps: department directors and other responsible management, information technology staff, system security administrator, representatives of different user groups, and legal counsel. Because of rapid advancements in technologies, keeping the security P&Ps viable for the long term necessitates flexibility. Therefore, to the extent possible, avoid drafting P&Ps that are dependent on specific hardware and software solutions; rather, clearly define the mechanisms and processes for updating the P&Ps.

Feds Target Growing MD Practices

continued from p. 1

Physicians may let their guard down because years of a war on health care fraud have brought large-scale enforcement actions only against other kinds of providers. Generally only physicians whose abuses were flagrant were prosecuted, but there have been relatively few settlements with physicians for offenses that equate to DRG upcoding and lab unbundling. "Many have enjoyed basking in the comfort of the fact that the False Claims Act has been out there in the health care arena for a long time and they don't know anyone hit except the really bad boys, and that didn't surprise them," says consultant Jim Stroud. "It's mistakenly given doctors a false sense of security. There's some real jeopardy for physicians."

Plus physicians feel they are working harder for less money, so some continue to adopt aggressive billing strategies they may hear about from a respected colleague on the golf course.

Whistleblowers are a potent risk to physician practices. When one person gets a lifetime earning stream for turning in the providers they work for, others begin to question their physician-employer's business and billing practices, says Stroud, with Warren, Averett, Kimbrough & Marino.

"If the government's goal is not just to disgorge money from the system but also to get compliant and correct coding and billing, it stands to reason they have to get to doctors," Stroud says. "If they can get to a few of the practices and acquaint them with the perils of making a mistake [in high-profile settlements], they get them to comply." While there's probably less money to recover from physicians than from institutions, false claims actions against practices send a message that doctors need to set up a system for preventing, detecting and correcting mistakes.

6 Strategies for Better Billing, Documentation

Complicating matters is the complexity of the Medicare billing rules for physician services, notably the evaluation and management levels of service. They are rife with opportunities for both upcoding and undercoding.

Here are some areas of physician billing that are prone to billing mistakes and suggestions for improving your billing, according to Lisa Warren, also a consultant with Warren, Averett, Kimbrough & Marino:

(1) Physicians tend to document patient histories incompletely. The history part of Medicare's evaluation and management documentation guidelines requires the history of present illness; review of systems; and medical, social and family history. Warren says that physicians, particularly surgeons, often fail to document the number of systems they review or don't conduct any of the 10 reviews of systems necessary to push the visit out of a level one. Physicians often don't jot down that the results of a review of a particular system were negative, even though they'd get credit for reviewing that system. If the cardiovascular system was negative, they can write "regular rate and rhythm" and get credit for reviewing that system. "Their failure to document the negatives means they are stuck with a level one because they are not hitting any of the bullets," Warren says.

(***2) Many physicians don't adequately document consults in the medical records.*** Warren says the consult codes call for the consulting physician to state explicitly that "this is a consult for Dr. Smith" — or it won't be considered a consult. "A lot of times physicians use consult codes, but there's no evidence in the dictation of who the consult was for," she says. Physicians should

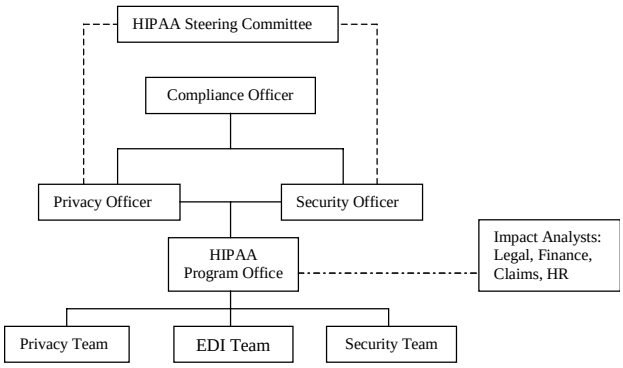
HIPAA Compliance: A Step-by-Step Guide, Part 3

Here is the third installment in our series on integrating HIPAA privacy and security requirements into your existing compliance program. The series is written by attorney Michael Bell. This week, he addresses the second element of a HIPAA compliance program: designation of privacy and security oversight responsibility. Contact Bell, who is with the law firm of Mintz, Levin, Cohn, Ferris, Glovsky & Popeo PC, at (202) 434-7481.

As the term "compliance officer" has become ubiquitous within the health industry's vernacular, so will the terms "privacy officer" and "security officer" in the years to come. Similar to the OIG's compliance program guidances, each of the HIPAA privacy and security regulations requires designation of oversight responsibility for the implementation and operation of the organization's privacy and security programs. Consequently, by the year 2003, every covered entity will have individuals and / or committees within the organization responsible for privacy and security compliance.

Creating Your HIPAA Infrastructure

Many health care entities already have established task forces or committees to evaluate and begin addressing HIPAA compliance.



The organization's board of directors or equivalent governing body should authorize the creation of HIPAA task forces or committees through a written resolution or directive. If your organization has not done so, or if you are evaluating the group you have selected, consider the following when assigning HIPAA oversight responsibility:

(1) Create a HIPAA reporting structure. Starting with the board of directors, or a sub-committee thereof, trace direct and indirect reporting relationships down throughout the organization. The above diagram illustrates a HIPAA reporting structure currently in place at one health care organization

Obviously, the size and precise structure of the program will differ across organizations and will depend on the availability of human resources.

(2) Define roles before assigning responsibilities. Define the roles and responsibilities of each of the boxes (positions) created in your HIPAA reporting structure. While this may seem obvious, often organizations assign the positions first then ascertain the duties. Start by creating a job description for both the Privacy Officer and Security Officer before assigning the positions. With HIPAA, it is important to understand the roles of these positions because they involve very different realms of knowledge.

The Privacy Officer's domain will include access to, uses, disclosures, and disposition of protected information, and will entail significant interaction and collaboration with department, committee and clinical personnel.

The Security Officer's domain, on the other hand, involves knowledge of network and enterprise-wide information systems and architecture, security threats and mechanisms, intrusion management, firewall administration, incident response, activity monitoring and auditing, and other technical details.

It is unlikely that an organization's Privacy Officer will have the skill set needed to be an effective Security Officer, and vice-versa. Identify the roles and responsibilities first, then determine the appropriate person for the job.

(3) Create winning teams. Each team or task force assembled should include representatives from each operational area / department within the organization. For many health care organizations, the teams should include interested representatives and / or subject matter experts from the following departments: patient admissions / registration; medical and clinical staff; finance; operations; sales and marketing; purchasing; legal; HR; information systems; records; risk management and compliance.

Take advantage of institutional memory, demonstrate commitment, and facilitate commitment of resources by assigning members of senior management to the HIPAA Program Office or equivalent committee.

Providers Are Behind In Assessing HIPAA Readiness

Health care organizations have less than 18 months to comply with HIPAA electronic transaction standards and less than 24 months for privacy regulation compliance, but most health care organizations have not finished a "gap analysis" of their privacy and security practices.

While many health care organizations are implementing some form of readiness plan, a survey conducted by Gartner, Inc. found that 75% of the 203 payer and provider health care organizations surveyed have not completed transaction assessments of their environments and risks.

The survey suggests that health care organizations aggressively begin compliance efforts within the next three months or run the risks associated with missing the deadline. The survey also found that: 27% of organizations have budgeted money for compliance measures; less than 30% have started compliance education programs; only 9% have completed privacy assessments; and 11% of health care organizations have started obtaining vendor contractual commitments for HIPAA compliance.

The survey also found payers way ahead of providers in HIPAA compliance. Four times as many payers have completed transaction and code set assessments and this could lead to communication problems even if a provider is compliant before the deadline.

But fortunately, at least half of the compliance officers surveyed report directly to their CEO or a senior management committee — so at least their concerns are being heard.

Visit www.gartner.com or call Danielle Westling at (203) 316-7654. ✧

HIPAA Compliance: A Step-by-Step Guide, Part 4

Here is the fourth installment in our series on integrating HIPAA privacy and security requirements into your existing compliance program. The series is written by attorney Michael Bell, with the Washington, D.C., offices of the law firm Mintz, Levin, Cohn, Ferris, Glovsky & Popeo PC. This week, he addresses training, the third element of a HIPAA compliance program. Contact Bell at (202) 434-7481.

Each of the proposed *Security Standards* and the final *Privacy Regulations* require covered entities to provide training regarding the protection of health information. While the content may be regulated, covered entities have considerable latitude in the design, structure and format of these training programs. Therefore, take advantage of your existing corporate compliance training regimen by creating general (for all employees) and specific (departmental and role / user-based) training modules for inclusion in the organization's general and specific compliance training programs.

Like compliance, HHS wants privacy and security awareness to be part of daily operations and office procedure, and even suggests that recurring discussion of these topics occur in staff meetings. Such routine, but informal, training is an excellent way to ingrain any new program into the fabric of operations. However, do not mistake an informal setting as an excuse not to collect training-related documentation—take credit for all of your compliance-related activities.

Document the following with regard to all such compliance-related training:

- Time and date;
- Names and positions of attendees;
- Name(s) of trainer;
- Topics discussed;

Materials presented, if any; and

- Duration.

Maintenance of complete records is critical to demonstrating compliance and the organization's commitment to the program.

With regard to the regulations, HHS removed from the final *Privacy Regulations* two significant training-related burdens: the requirement for employees to complete a certification following training and triennial certification requirement. Only time will tell if HHS will soften the training requirements set forth in the proposed *Security Standards,* which are specific and broad in scope (requiring training for employees, agents, and contractors).

The following chart sets forth the training requirements under both the final *Privacy Regulations* and the proposed *Security Standards*, and should be useful as you develop and modify your organization's training programs.

Training Elements	Privacy	Security (Proposed)
What are the content requirements?	In the comment section to the final regulations, HHS provides that it does not "prescribe the content of the required training; the nature of the training program is left to the discretion of the covered entity." Notwithstanding, the regulations provide that training must cover the policies and procedures that were drafted to comply with the regulations, "as necessary and appropriate for the members of the workforce to carry out their function within the covered entity."	Education concerning the vulnerabilities and methods for ensuring protection of health information, including: **Security Awareness Training**, including password maintenance, incident reporting, viruses, malicious software; access requirements; termination of access for individuals who no longer have a need for such access. Although not specifically required, address: contingency planning, physical security; and records processing. **Periodic Security Reminder**s-provide information regarding security concerns on an ongoing basis. **Virus Protection**-"[t]raining relative to user awareness of the potential harm that can be caused by a virus, how to prevent the introduction of a virus to a computer system, and what to do if a virus is detected." **Monitoring Log-In Success Or Failures and How To Report Discrepancies** -identification of log-in/access issues and anomalies and the reporting of same. **Password Management**-confidentiality of passwords; and the rules to be followed in creating and changing PINs, passwords, and other private access codes.
Are there format requirements?	No. HHS recognizes that training methods might include classroom instruction, videos, video conferences, computer based training, booklets, or brochures tailored to particular levels of need of workers and employers. Interestingly, HHS based its costs estimates for training on one hour of training and a class size of ten.	No. In Addendum 2, a glossary to the to the proposed regulations, HHS provides a definition of **Awareness Training** that includes, "based on job responsibilities, customized education programs that focus on issues regarding use of health information and responsibilities regarding confidentiality and security." HHS also offers that **Periodic Security Reminders** "could include visual aids, such as posters and screen savers."
Who must be trained?	The regulation makes the following two references. First, the standard provides that a covered entity must train "all members of its workforce…as necessary and appropriate for the members of the workforce to carry out their function within the covered entity." The implementation specification states, "[t]o each member of the covered entity's workforce." In the preamble, however, HHS states that "the final rule requires all employees who are likely to have contact with protected health information to be trained." Guidance from HHS is forthcoming that may clarify privacy training requirements.	For **Awareness training**, "all personnel, including management" must receive training. **Periodic Security Reminders** must be provided to "employees, agents, and contractors." Although the term "personnel" is not specifically defined in the proposed regulations, Addendum 2 provides with regard to **Awareness Training** that "all employees, agents, and contractors must participate, including, based on job responsibilities, customized educational programs that focus on issues regarding use of health information and responsibilities regarding confidentiality and security."
When must training occur?	Each member of the covered entity's workforce must receive training no later than April 14, 2003 (except for small health plans, which have until April 14, 2004). Each new member of the workforce must receive privacy training within a reasonable period of time after the person joins the covered entity's workforce. Also, if there is a "material change" in the covered entities policies and procedures, each member of the workforce affected by the change must receive training within a reasonable period of time after the material change becomes effective.	Within two years of the effective date of the final regulations (yet to be released). The preamble also provides that "Security Awareness Training would be part of the new employee orientation process and would be a periodic recurring discussion item in staff meetings."
How often must training occur?	There are no express training frequency requirements Note that the requirement that training occur every three years has been dropped from the final rule. Retraining is only required in the case of material changes to the privacy policies and procedures of the covered entity.	There are no express training frequency requirements. Note, however, that **Periodic Security Reminders** must be issued and the HHS contemplates that training will occur during employee orientation and during staff meetings.
Documentation requirements	Covered entities must document that the required training has been provided. Note that the requirement for signed training certifications has been eliminated.	The proposed regulations required documented, formal practices for security training.

HIPAA Compliance: A Step-by-Step Guide, Part Five

Here is the fifth installment in our series on integrating HIPAA privacy and security requirements into your existing compliance program. The series is written by Michael Bell, with the Washington, D.C., offices of the law firm Mintz, Levin, Cohn, Ferris, Glovsky & Popeo PC. This week, he addresses reporting, the fourth element of a HIPAA compliance program. Contact Bell at (202) 434-7481.

The past several articles discussed the practicability of using your corporate compliance program infrastructure as a vehicle or model for the development and implementation of your HIPAA privacy and security programs. In this article, we discuss the analogues to the compliance program requirement for "having in place and publicizing a reporting system whereby employees and other agents could report criminal conduct by others within the organization without fear of retribution," otherwise known as a compliance hotline. Each of the Privacy Regulations and the proposed Security Standard call for reporting mechanisms, but these requirements are different from each other and from a traditional compliance hotline in significant ways.

Unlike the seven elements of an effective compliance program, which require lines of communications for *agents and employees* to report suspected violations, the Privacy Regulations require covered entities to provide a process for an "individual," which is defined as the person who is the subject of the protected health information, to submit complaints to the covered entity. As discussed in greater detail below, it is recommended that covered entities encourage employee reporting of privacy issues, though the reporting-related requirements contained in Privacy Regulations focus on reports, or complaints, by the individual.

The complaint reporting requirement arises in four different contexts within the Privacy Regulations. First, covered entities must include within their *Notice of Privacy Practices* a statement that individuals may complain to the covered entity and / or to the Secretary "if they believe that their privacy rights have been violated." The *Notice* also must include a statement that the individual will not be retaliated against for making the complaint.

Second, covered entities must provide "a process for individuals to make complaints" to the covered entity concerning the covered entity's policies and procedures, compliance therewith, or compliance with the Privacy Regulations generally. This second requirement affords individuals an avenue to report complaints about conduct unrelated to either the regulations or their own protected health information. The preamble to the regulations offers the following by way of example: "a covered entity must have a mechanism for receiving a complaint that patient information is used at a nursing station in a way that it can also be viewed by visitors to the hospital, regardless of whether the practices at the nursing stations might constitute a violation of this rule."

Although the preamble discussion of the *Notice* requirement references the *process* requirement, the text of the regulations themselves does not. While the distinction between these two requirements is subtle and may be irrelevant in many circumstances, it remains that covered entities need not include in their *Notice of Privacy Practices* a statement that individuals may submit complaints for anything other that perceived privacy rights violations. Rather, individuals who want to make a complaint must be provided a process with which to do so. Many health care organization may wish to inform (through the *Notice*) individuals of their ability to submit any privacy-related concern, though the regulations require only that the covered entity inform of their right to submit a complaint "if they believe that their privacy rights have been violated."

You Must Explain Complaint Procedures

In addition to the *Notice* requirement described above, covered entities also must provide individuals with information regarding complaint procedures both to the covered entity and to the Secretary if and when the covered entity denies, in whole or in part, an individual's request for either access to or amendment of his or her protected health information.

Descriptions of the complaint process required by the regulations must include the name, or title, and the telephone number of a person or office to contact for further information about matters covered by the *Notice.* Covered entities must also maintain a detailed log of complaints and their resolutions, if any. Organizations that meet the requirements of an "Affiliated Entity" or an "Organized Health Care Arrangement" may, in addition to other efficiencies, appoint a single contact person or office to receive complaints.

Although the regulations require only a process for individuals to submit complaints, there are several

reasons supporting the expansion of the internal reporting system to all employees and agents of the covered entity. First, covered entities are responsible for the actions of their business associates, and although covered entities don't need to actively monitor their business associates, "a covered entity nonetheless is expected to investigate when they receive complaints or other information that contain substantial and credible evidence of violations by a business associate, and it must act upon any knowledge of such violation that it possesses."

Second, the final Privacy Regulations expressly permit employees to make complaints regarding violations to the Secretary and affords protections for whistleblowers. Thus, from both a compliance and a liability standpoint, it is prudent for a covered entity to make available, and moreover encourage, the use of internal reporting by employees, agents and business associates of the covered entities.

Expansion of the requirements results in only marginal increases in implementation efforts. Covered entities should consider simply using their existing compliance hotline to respond to privacy related complaints. Likewise, existing reporting policies and procedures may be amended to address privacy complaint reporting. Internal and external hotline intake personnel already are trained in handling such matters and need only receive guidance relative to the reporting hierarchy of the privacy program to the extent it differs from the compliance program.

The proposed Security Standard also contains a reporting requirement. The proposed regulations would require covered entities to implement security incident report and response procedures, which are "formal, documented instructions for reporting security breaches, so that security violations are reported and handled promptly." While many organizations already have in place policies and procedures addressing this very topic, in many cases they are issued once without further ongoing education, and consequently, these policies and procedures fade from memory. Here, the key is promoting employee awareness and recognition of potential breaches in physical and technical security.

Proper internal reporting of security incidents is critically important to a health care organization. Prompt and efficient reporting and response will protect from improper disclosure of health information, and will preserve company assets and resources, and may prevent the use of the organization's systems for attacks against other systems. Indeed, incident reporting reduces legal liability and curbs the potential for bad publicity and loss of customer confidence.

Covered entities' policies and procedures should address several layers of reporting. As time is of the essence in a security breach, employees and agents should be told to contact the Security Officer or his/her designees immediately upon suspecting a potential breach. Subsequent layers include reporting between the Security Officer and the Compliance Officer and legal counsel; communications with administrators and directors; and carefully considered communications with business associates and other third parties.

Hospitals Can Rebill Discharges

continued from p. 1

Can you fix these errors and recoup your reimbursement at any time, even years later? Yoe says yes, and explains that his position is clearly supported by Medicare manuals. Plus he says that several fiscal intermediaries acknowledge there is a four-year or no time limit on resubmitting claims to Medicare to get more money for the discharged patients who were billed as transfers. But at least one intermediary and a major HCFA regional office insist there is a 60-day cap on fixing patient status code errors, and is rejecting claims resubmitted by hospitals with corrected patient status codes. "There's inconsistent treatment by the fiscal intermediaries," he says. Some assert there's no time limit, others say four years — "but I've never had one say it's 60 days."

Here's how this issue arises: If a patient is transferred from a prospective-payment system hospital to a non-PPS facility (i.e., rehab, psych), the hospital should bill that encounter as a discharge — except for 10 DRGs that must be billed as transfers when followed by post-acute care *(RMC 3/15/01, p. 1)*. The claim should show a discharge disposition code that represents the kind of facility the patient is being discharged to, Yoe says. Otherwise, if the patient is being sent from a PPS facility to another PPS facility, the claim should have the patient status code 02, which tells HCFA to pay for a transfer.

"In some cases, the medical record cover sheet will indicate that the patient was transferred, but will not indicate what type of facility that patient was transferred to. In these cases, the billing personnel may erroneously assign patient status code 02 to the claim," Yoe says. "Because of the incorrect information it has received, the fiscal intermediary will pay the claim as a transfer."

continued

because providers have to have IROs do their auditing and monitoring, so they typically retain a consulting firm and pay a lot of money for that process," notes attorney Paul DeMuro.

Meanwhile, the OIG is separately considering whether to ease that requirement.

Organizations that self-disclose their violations almost always get a better deal on their CIAs from the OIG. Some examples, which appeared in the report:

"(1) A rural hospital in the Southeast self-reported that, while under former ownership and management, it had submitted claims with information that was falsified to support reimbursement. The hospital uncovered the false claims during the course of an internal audit performed as part of its voluntary compliance program. In the fall of 2000, the hospital agreed to resolve its financial and exclusion liability. The OIG did not impose a CIA because the misconduct was committed by the former management and the new management disclosed its findings to the Government as part of a comprehensive pre-existing compliance program.

(2) An acute care hospital in the Southwest — one of several nonprofit affiliates of a larger health system — identified that it had improperly coded claims to the Federal health care programs for mammography services. The hospital uncovered the false claims during the course of an internal audit performed as part of its voluntary compliance program. In the summer of 2000, the

HIPAA Compliance: A Step-by-Step Guide, Part 6

Here is the sixth installment in our series on integrating HIPAA privacy and security requirements into your existing compliance program. The series is written by Michael Bell, with the Washington, D.C., offices of the law firm Mintz, Levin, Cohn, Ferris, Glovsky & Popeo PC. This week, he addresses sanctions, the fifth element of a HIPAA compliance program. Contact Bell at (202) 434-7481.

Both the Privacy Regulations and the proposed Security Standards require covered entities to impose sanctions for violations of law or policy. This is a straightforward requirement, and most, if not all, health care organizations already maintain disciplinary policies and procedures for inappropriate work place behavior and / or compliance program violations. While an HR and / or compliance policy simply may be amended to address privacy and security violations, proper administration of the policy, which will both afford protection in employment-related disputes and evidence an effective compliance program, requires sufficient notice, consistent and fair application, and documentation.

Generally, organizations should clearly communicate, both orally and in writing, the sanctions policy to the workforce. Create and / or amend existing policies and procedures (P&Ps) and training modules to state clearly that violations of the privacy and security procedures will result in corrective action, which may range from verbal warning and retraining for unintentional acts or omissions to termination for intentional or repeated and systematic violations. Build flexibility into the policy and consider requiring employees and agents to sign a statement acknowledging that they have read and understand the P&Ps and that violations will result in disciplinary action. Include periodic policy reminders on employee bulletin boards, and in mailings and newsletters. Also, promotion of and adherence to the P&Ps should be a factor in the performance evaluation of employees, supervisors and managers.

Specifically, the Privacy Regulations require covered entities to apply and document "appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures" or the regulations. The proposed Security Standards require the same, but also require covered entities to inform employees, agents and contractors that misuse or misappropriation and other violations may result in civil or criminal penalties and / or "notification to law enforcement officials and regulatory, accreditation, and licensure organizations."

To avoid and minimize the consequences of employment-related disputes, administer corrective action consistently without regard to rank or status. The corrective actions initiated should be progressive as well as reasonable and commensurate to the violations. In addition to typical sanctions — verbal warning through termination — covered entities may employ system-related penalties such as removal of user account(s), system privileges and / or employee "perks."

Thoroughly document corrective or disciplinary actions taken pursuant to the policy. Finally, retain documents related to such actions in employees' HR files or contract files / binders for at least 6 years and 10 years (after termination of the contract), respectively.

Dark Side of Compliance

continued from p. 1

Compliance officers "are only as good as the data they are given," he says.

Second-Guessing Your Own Reality

How can you tell whether you have adequate power, resources, respect and independence to be an effective compliance officer? Take what we call the mushroom challenge. Compliance officers should not be like mushrooms, which are kept in the dark and fed manure to grow, says Kimble Carter, an attorney who is Director of Compliance for the South Carolina Department of Mental Health.

Carter devised these questions to help you evaluate whether you have more in common with a mushroom than you should — or whether you, as a compliance officer, are sufficiently empowered to make tough calls and bring bad news to management, and are privy to sensitive documents, included in important decisions and tackle tough issues affecting the organization.

Are you:

◆ Kept in the dark, or involved in important discussions / decisions?

◆ Fed information or do you have unlimited access to it?

◆ Cut to pieces or chewed out when you find a major problem, or are you given the resources to thoroughly address the problem?

HIPAA Compliance: A Step-by-Step Guide, Part 7

Here is the seventh installment of our series on integrating HIPAA privacy and security requirements into your existing compliance program. The series is written by Michael Bell, with the Washington, D.C., offices of the law firm Mintz, Levin, Cohn, Ferris, Glovsky & Popeo PC. This week, he addresses audits, monitoring and accounting, the sixth element of a HIPAA compliance program. Contact Bell at (202) 434-7481.

While the Privacy Regulations, unlike the compliance program elements, do not require explicit auditing, as set forth in the chart on p. 7, the Privacy Regulations do require covered entities to track certain non-routine disclosures of protected health information (PHI) and to provide individuals with an accounting of these disclosures. Despite the absence of an express audit requirement, it is prudent for health care organizations to periodically audit and monitor its compliance with the Privacy Regulations. To assess and demonstrate compliance with the numerous HIPAA-related requirements, covered entities will need to review and document their compliance with various aspects of the regulations (*e.g.*, minimum necessary, consents and authorizations, business associate agreements, etc.).

The proposed Security Standard, on the other hand, mandates technical auditing capability and the performance of ongoing audits of system activity. The preamble to the proposed regulations states, "[e]ach organization would be required to put in place audit control mechanisms to record and examine system activity. They would be important so that the organization can identify suspect data access activities, assess its security program, and respond to potential weaknesses." In addition, if the covered entity transmits health information over an open network, it must also maintain an "audit trail," which generally is a record of each time a document is accessed, altered, how it was altered, and by whom. Many health care organizations already maintain systems and software capable of satisfying these security audit requirements.

The audit data collected pursuant to a security audit will differ for different sites and types of access changes within a covered entity, and should reflect the organization's attempts to achieve layered security levels. Generally, health care organizations should collect the following information for a security audit: logins and logouts; usernames and hostnames; old and new access rights; changes in access rights; file accesses; timestamps; and security incidents. Do not, however, collect passwords as this creates a great potential for a security breach. Covered entities may wish to test the security of their systems by attempting to gain access from an external computer and without proper system authorization. Such "ethical hacking" may reveal weaknesses in the security structure.

The audit data should be carefully secured and, in the event of a detected security incident, maintained in such a manner so as to both assist in the investigation and be admissible in the prosecution of the intruder / hacker. Also, as the audit data may contain PHI, it is important for covered entities to consider the "minimum necessary" standard of the Privacy Regulations when developing the organization's audit policy.

◆ Told what happens at significant internal meetings or are you a member / chair?

◆ Meeting with important external parties (attorney general, carrier reps) or not?

◆ Communicating with the CEO and board through others (hence, everything is filtered) or personally?

◆ In a relatively secure position because of contract / grievance rights, or are you subject to your boss' whim?

◆ Only conducting educational programs or are you involved in all aspects of the compliance program?

◆ Automatically provided with audits by other divisions and outside auditors, or do you have to beg for them?

◆ An afterthought when the big one hits, or the first one the CEO calls?

◆ Having your concerns buried in subcommittee and interminable review processes, or having assistance in cutting to the chase?

◆ Not appreciated for getting your organization ahead of the curve in relation to recently developed and developing accreditation standards — or given kudos?

◆ Denied necessary budgetary requests or, at least, given partial good-faith funding?

◆ Only getting results when you bring in the boss, or are most staff providing appropriate, timely responses to your requests?

◆ Having a hard time getting a quorum at your compliance meetings, or do people come and join in meaningful discussions?

◆ Seeing supervisors not dealing with employees who engage in noncompliant activity, or are they taking appropriate disciplinary actions?

◆ Finding that the chain of command is primarily interested in figuring out the identity of the anonymous whistleblower — or are you finding they mainly want to know whether the allegations have merit?

◆ Interviewing for a compliance position, and your potential boss is not the CEO? And the interviewer / non-CEO leaves no doubt that you must clear all issues with him / her and not bother the CEO? And you find out the organization is hiring a CCO primarily because of an

Accounting for Disclosures of PHI (continued from p. 6)

Are all covered entities subject to this requirement?	Generally, no-while providers and health plans will be required to provide an accounting of disclosures, clearinghouses that are acting as a business associate will not be subject to this requirement.
What disclosures are subject to the accounting requirement?	All disclosures, including disclosures made by business associates, other than those made for treatment, payment, or health care operations made after April 14, 2003 (April 14, 2004 for small health plans), except for disclosures: to the individual; for the facility's directory; to persons involved in the individual's care; for national security or intelligence purposes; or to correctional institutions or law enforcement officials.
How many years must an accounting of disclosures cover?	6 years from the date of the request. Note, however, that the requirement applies only to disclosures made after the compliance date. What must the accounting include? 1. the date of the disclosure; 2. the name of the entity or person who received the PHI; 3. the address of the entity or person who received the PHI, if known; 4. a brief description of the PHI disclosed; and 5. a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or alternatively, a copy of the individual's written authorization, a copy of a written request for a disclosure made by the Secretary for purposes of assessing a covered entity's compliance with the regulations, or a copy of a written request for a disclosure made by an individual or entity for which no consent or authorization to disclose was needed. (Note that different rules apply to multiple disclosures made to the same individual or entity for a single purpose pursuant to these latter two purposes need.)
When must an accounting be provided?	A covered entity must act on the individual's request for an accounting no later than 60 days after receipt of such a request. Covered entities may extend this time limit one time for thirty days if the covered entity provides the individual with reasons for the delay and the date by which the covered entity will provide the accounting.
May a covered entity charge the individual for the accounting?	The first accounting within any 12 month period must be provided free of charge. The covered entity may charge a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided that the covered entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.
What are the compliance documentation requirements?	For a period of at least six years, the covered entity must maintain: 1. the information required to be included in an accounting; 2. the written accounting that is provided to the individual; and 3. the titles of the persons or offices responsible for receiving and processing requests for an accounting.
SOURCE: Attorney Michael Bell, (202) 434-7481.	

HIPAA Compliance: A Step-by-Step Guide, Part 8

Here is the last installment in our series on integrating HIPAA privacy and security requirements into your existing compliance program. This week's article focuses on the seventh element of a HIPAA compliance program: responding to incidents. The series is written by attorney Mike Bell, with the Washington, D.C., offices of the law firm Mintz Levin Cohn Ferris Glovky &Popeo PC. Contact Bell at (202) 434-7481.

While no element of a compliance program is more important than another, a true test of the program's effectiveness (and the organization's commitment to its compliance program) is how the organization addresses its own potential violations of law and / or policy. It is expected that all health care organizations will make mistakes — how those mistakes are handled, however, is truly revealing. The seventh and final element of an effective compliance program provides that "[a]fter an offense has been detected, the organization must have taken all reasonable steps to respond appropriately to the offense and to prevent further similar offenses — including any necessary modifications to its program to prevent and detect violations of law." As with virtually every other element of the Guidelines, this concept of corrective action has been modified and incorporated into the Privacy Regulations and the proposed Security Standard alike.

Striking a compromise between the positions taken by privacy advocates and by the health care industry, the Department of Health and Human Services ("HHS") created what is, from a legal perspective, easily one of the more interesting provisions in the Privacy Regulations. Specifically, the Privacy Regulations create a duty for covered entities to "mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of [the Privacy Regulations] by the covered entity or its business associate."

While HHS provides on two occasions in the final rule that the duty is triggered when the covered entity has actual knowledge of harm that will result from the disclosure, the prudent course of action for a health care provider would be to assess the sensitivity of the information disclosed and to make an informed determination as to what, if any, actions should be taken to mitigate the actual and potential harmful effects of the disclosure.

Unlike a simple billing error where a health care organization's options for corrective action are relatively straight-forward (e.g., resubmit the claim or refund the overpayment, change the policy or system or retrain, if necessary), appropriate mitigation of a harmful disclosure of PHI is less clear. Improper and harmful uses or disclosures should be a rare occurrence; consequently, covered entities should address such situations on a case-by-case basis pursuant to established and defined guidelines. Despite the individual nature of the assessment, covered entities are well-advised to develop written policies and procedures by which to evaluate and employ various corrective actions. Note that privacy-related mitigation policies and procedures could be appended to or modeled after existing compliance program policies and procedures.

The manner by which a covered entity attempts to mitigate the deleterious effect of an improper use or disclosure should reflect a thorough assessment of the following factors:

(i) The nature and the sensitivity of the information;

(ii) The nature of the harm;

(iii) The number of persons who received or obtained improperly the PHI;

(iv) The relationship, if any, between the individual and the receiver of PHI;

(v) The intended purpose of the use or disclosure; and

(vi) The method of the use or disclosure. Appropriate mitigating actions may range from retrieval of the information and distribution of a carefully crafted notice to the recipient to exercising contractual remedies. This latter option highlights the importance of well drafted business associate agreements, as it is the covered entity that is ultimately responsible for the actions of its business associates.

In this regard, covered entities are required to take reasonable steps to remedy known breaches or violations of their business associates' obligations. The preamble to the final rule provides that covered entities are "expected to investigate when they receive complaints or other information that contain substantial and credible evidence of violations by a business associate, and it must act upon any knowledge of such violation that it possesses." If a covered entity is unable to remedy the violation and the business associate can not be relied upon to protect PHI, it must terminate the arrangement with the business associ-

ate, if feasible, or if termination of the arrangement is not feasible, the covered entity must report the problem to HHS.

Although it is unclear how HHS will handle such reports, it is significant to note that the penalties provisions of the statute apply not only to covered entities, but to any individual or entity that wrongfully obtains or discloses individually identifiable health information.

Finally, while the rule requires mitigation "to the extent practicable"; it does not require covered entities to eliminate the harm in all circumstances. HHS offers the following by way of example: "if protected health information is inadvertently provided to a third party without authorization in a domestic abuse situation, the covered entity would be expected to promptly contact the patient as well as appropriate authorities and apprise them of the potential danger."

The proposed Security Standard also requires covered entities to take appropriate action to cure security breaches or other known security issues. Specifically, the proposed rule calls for incident response procedures, which are "documented formal rules or instructions for actions to be taken as a result of the receipt of a security incident report." Similarly, the proposed Security Standard requires covered entities to develop: a contingency plan for responding to emergencies; a data backup plan; a disaster recovery plan; and an emergency mode operation plan.

Goals of an Incident Response Procedure

Generally, the objectives of security incident response procedures are as follows

(i) Determine the cause of the breach;

(ii) Determine means to contain the problem and avoid escalation and further exploitation of the vulnerability;

(iii) Assess the impact of the incident;

(iv) Eradicate the cause;

(v) Employ recovery plans;

(vi) Update / revise policies and procedures and / or system configuration;

(vii) Monitor for latent holes or traps; and, if feasible; and

(viii) Identify the intruder. Incident response procedures should contain well-defined policies and goals, and should be periodically tested to ensure their effectiveness.

Be sure to contact legal counsel as soon as you become aware that an incident is in progress so as to minimize or avoid downstream liabilities that may arise from: damage to another system caused by your system, economically damaging disclosures about software or systems, improper monitoring of system activity, and other unforeseen issues. Moreover, legal counsel should be involved to protect potential evidence and activity logs for purposes of investigation and prosecution of the intruder(s).

NEWS BRIEFS

◆ **More answers to more questions about Medicare's home health PPS that were posed by the industry have been posted on the HCFA Web site** at www.hcfa.gov / medlearn / refhha.htm. Warning: finding the latest questions and answers is a little confusing: click on the "RTF version" links next to the files labeled December 2000 — January 2001 Batch 2 and January 2001 Batch 3. The original answer set which was posted in March is now labeled Batch 1. "We are continuing to work on the backlog of inquiries to this mailbox and hope to post replies to all inquiries received in February and March 2001 in coming weeks," HCFA says.

◆ **Want to get a sense of the intensity and scope of recent HHS Inspector General Medicare-Medicaid fraud policing efforts?** The latest semi-annual report for the six-month period ending March has been posted on the OIG Web site at www.hhs.gov / oig.

◆ **HCFA has posted a corrected PC version of the Medicare pricer software for home health claims to solve problems being experienced by new enrollees and for entities that don't have their own provider numbers.** The corrected software can be downloaded from the HCFA Web site at www.hcfa.gov / medicare / nm75ght / pricdnld.htm. HCFA instructs users to download the version of the Home Health PPS Pricer marked "Posted May, 24, 2001." When opening the zipped file, save to the default C: drive to the default