Learn from others’ mistakes  

Common deficiencies targeted in OCR corrective action plans

There is some common ground in the corrective action plans (CAP) that OCR has imposed on healthcare organizations it has investigated for HIPAA privacy and security deficiencies.

Since the first settlement in 2008, OCR has reached resolution agreements and CAPs with 14 organizations, the latest one occurring in June (as of BOH press time in July; see related story on p. 4). Healthcare organizations can gain tremendous insight into how they can improve their culture of compliance when it comes to privacy, security, and breaches by looking at these CAPs and how OCR has adjudicated the investigations, said David Ginsberg, cochairman of the Workgroup for Electronic Data Exchange (WEDI) privacy and security workgroup, and cofounder and president of PrivaPlan Associates, Inc., in Santa Fe, N.M. Ginsberg was a speaker during the June 14 webinar “HITECH Omnibus Overview of the Rule”—the first in a series of events sponsored by OCR and WEDI to educate organizations about changes under the final rule.

There are some common gaps and deficiencies found in healthcare organizations that are apparent in the CAPs, Ginsberg said. You can find a comparative analysis of the HIPAA deficiencies noted in the CAPs, as well as information on upcoming webinars, on the WEDI website at www.wedi.org.

Based on those CAPs, the following are some areas healthcare...
OIG: Medicare contractor exposed personal information of beneficiaries

Personally identifiable information of more than 6 million Medicare beneficiaries was compromised because of a government contractor’s lack of adequate security controls for USB devices, according to an Office of Inspector General (OIG) report released in June. OIG assessed the USB device controls at Quality Software Services, Inc. (QSSI), the contractor responsible for testing changes to the CMS Medicare systems and the effect of those changes on beneficiary data. OIG found QSSI had not sufficiently implemented federal requirements for information system security controls over USB ports and devices because QSSI had not listed essential system services or ports in its system security plan. QSSI also failed to disable, prohibit, or restrict the use of unauthorized USB device access. OIG recommended that QSSI update and implement sufficient policies and procedures to ensure that USB controls comply with federal requirements.

http://blogs.hcpro.com/hipaa

FROM THE FIELD

“We always say that policies and procedures can’t be binders up on a shelf.”

Rachel Seeger

“This is the time to capitalize on your mental Rolodex. If you have a question on ‘X’, get these people in a room and let them help you nail down your process.”

Frank Ruelas, MBA

STAY CONNECTED

BOH in Your Inbox

Sign up for any of our 17 email newsletters, covering a variety of healthcare compliance, management, and reimbursement topics, at www.hcmarketplace.com.

Don’t miss your next issue

If it’s been more than six months since you purchased or renewed your subscription to Briefings on HIPAA, be sure to check your envelope for your renewal notice or call customer service at 800-650-6787. Renew your subscription early to lock in the current price.

Relocating? Taking a new job?

If you’re relocating or taking a new job and would like to continue receiving Briefings on HIPAA, you are eligible for a free trial subscription. Contact customer service with your moving information at 800-650-6787. At the time of your call, please share with us the name of your replacement.

Questions? Comments? Ideas?

Contact Editor Jaclyn Fitzgerald at jfitzgerald@hcpro.com or 781-639-1872, Ext. 3729.
organizations should focus on.

**Risk analysis**

The Security Rule requires organizations to conduct a HIPAA security risk analysis, but many have gotten into trouble for failing to conduct this analysis or conducting one that is insufficient.

It’s not only a weakness highlighted in CAPs, but also a common deficiency in recent OCR audits, Ginsberg noted. “It’s not a trivial task. It’s not a simple task, but it doesn’t have to overwhelm an organization,” he said. OCR has produced a guidance document on how to conduct a security risk analysis, he noted. You can find that guidance at [www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rationalguidancepdf.pdf](http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rationalguidancepdf.pdf).

With the release of the final rule, business associates (BA) are now subject to the HIPAA Security Rule and must also conduct a risk analysis, he said.

As part of conducting a risk analysis, organizations need to document what they have done, said Mark Cone, who cochairs the WEDI privacy and security workgroup with Ginsberg and also spoke during the webinar. Cone is a founder of N-Tegrity Solution Group and works out of its Blue Springs, Mo., office. “Put hard copy documentation in place to show what you did,” he said.

Cone said he has worked with a lot of organizations that have not documented their risk analysis process to show they understand their security vulnerabilities. For instance, if an organization allows outside entry into its computer systems, does that create vulnerability in terms of its technical infrastructure?

For organizations seeking CMS electronic health record (EHR) eligibility for meaningful use incentives, a risk analysis is also required, Ginsberg said. Going through a simple checklist is not a risk analysis and does not provide sufficient documentation, he noted.

**Training**

The need for more workforce training is a key finding in almost every CAP, said Ginsberg.

Lack of training prior to allowing staff to access PHI is a common problem. A CAP put in place with Massachusetts General Hospital in Boston requires the hospital to train new members of the workforce who have access to and use PHI within 15 days of beginning their service. That’s a benchmark for others, Ginsberg said.

Don’t provide cursory training without follow-up, he said. Failing to sufficiently customize training to your organization’s actual practices is also a problem.

Training should include all workforce members. The most recent CAP that was part of the settlement with Shasta Regional Medical Center in Redding, Calif., demonstrates that perhaps the organization’s leaders were not sufficiently trained on protecting patient PHI, Ginsberg said. In that case, senior leaders were responsible for the release of PHI to the media.

Lack of training on security procedures, including proper remote access and use, is another weakness. Train your workforce on security awareness and provide periodic reminders, Ginsberg said. Lack of training on mobile device access is also problematic in many organizations.

Finally, organizations often fail to provide training that is specific to workforce members’ roles and job duties. A standard “HIPAA 101” training program won’t cut it, Ginsberg said. In a physician practice, for instance, you may need to provide more extensive training to personnel in your back office who work extensively with your medical records, including referrals and authorizations, he said.

**Mobile and portable device safeguards**

A common problem in healthcare is a lack of risk analysis and management for mobile/portable devices that access, create, maintain, or transmit ePHI.

Think about the use of smartphones and computer tablets by your workforce, as well as laptop computers. Most EHRs have interfaces with tablets, which are becoming the most common data input device for healthcare workers because of their long battery life and ease of use, Ginsberg said.

A big problem is inadequate or nonexistent safeguards and controls for mobile devices. Too many organizations either have few or no policies and procedures to manage these devices, he said.

The failure to recognize and implement encryption and to secure transmission of PHI via texting and email are major weaknesses. Organizations that look at the risks created by these devices may decide to encrypt them or develop the capability to remotely wipe them clean of information if they are lost.
Devices can store hundreds of emails and contain a long trail of text messages that can include PHI. If they are lost or stolen, organizations are at risk for a breach, Ginsberg said.

Many organizations allow workforce members to connect their personal devices to the organization’s wireless network, said Cone. “It requires another level of security you need to be aware of,” he said, and should prompt the writing of a so-called bring your own device (BYOD) policy.

Organizations also need to think about the vendors they work with, such as those who have third-party applications hosted in the cloud, Cone said. You need to know if your organization’s data is hosted in a public or private cloud. For example, one organization believed it had no PHI stored on any of its desktop computers, until it realized that screenshots containing PHI had been sent to the help desk system and were stored on the open network.

**HIPAA administrative privacy and security gaps**

One failure of many organizations is their incident response and reporting policies and procedures, said Ginsberg. Some organizations sport stale, decade-old policies and procedures that need to be updated.

Another problem is that organizations have not implemented sanctions for dealing with workforce members who violate HIPAA policies and procedures. You need to establish and enforce these sanctions, he said.

Workstation use procedures are another weakness. Are your computer screens positioned so that someone casually walking by cannot see any PHI? Are staff trained to be aware of someone looking over their shoulder to view PHI when they are using a portable device at a coffee shop or even at home? Take steps to ensure that you are not allowing a passerby to catch a glimpse of PHI.

---

**Two more enforcement actions in 2013**

**HIPAA deficiencies cost healthcare organizations $15.75 million**

HIPAA privacy and security deficiencies have cost healthcare organizations $15.75 million in civil monetary penalties and resolution agreements with OCR.

OCR has entered into two more resolution agreements with healthcare organizations to settle potential violations of HIPAA this year—bringing the total number of resolution agreements to 14 since the first occurrence in July 2008 (as of BOH press time in July).

The June resolution agreement and corrective action plan (CAP) included a $275,000 monetary settlement by a California medical center. What was perhaps most surprising about the case, though, was that it involved the organization’s senior leaders.

Rachel Seeger, OCR’s senior health information privacy outreach specialist, announced news of the agreement June 14 in the first of OCR’s joint webinars with the Workgroup for Electronic Data Exchange SNIP Privacy and Security Workgroup to educate organizations about the omnibus final rule.

**What happened at Shasta**

OCR launched an investigation of Shasta Regional Medical Center in Redding, Calif., after a *Los Angeles Times* article indicated two senior leaders met with the media and discussed medical services provided to a patient, Seeger said during the webinar. The investigation revealed that Shasta failed to safeguard the patient’s PHI from impermissible disclosure by intentionally disclosing PHI to multiple media outlets on at least three separate occasions without valid written authorization, according to OCR.

The *Times* article appeared January 4, and OCR notified Shasta January 6 that it was starting a compliance review of its facility. OCR’s review also found that senior management at Shasta impermissibly shared details about the patient’s medical condition, diagnosis, and treatment in an email to the entire workforce. Shasta failed to sanction its workforce members for impermissibly disclosing the patient’s records pursuant to its internal policy.

The one-year CAP reached with Shasta requires the medical center to update its policies and procedures on safeguarding PHI from impermissible uses and disclosures and to train its workforce members on these policies and procedures. The CAP also requires 15 other hospitals or medical centers under
Weaknesses demonstrated by the CAPs include a lack of device security, facility controls and safeguards, secure handling and transporting of PHI, proper disposal of PHI, and proper media controls, including the storage of unencrypted ePHI.

Organizations need to define what qualifies as a privacy or security “incident,” said Cone. They need to ensure workforce members are not sharing passwords and that they have authentication controls. Log security incidents and document what you have done to mitigate problems.

If you are audited, you will need to show what you did to manage risks. It may be necessary to change your policies and procedures and then retrain your workforce, he said.

The CAPs reveal some other organizational weaknesses. Organizations need to be ready to respond to OCR investigations, said Ginsberg. “We believe this is critical,” he said. You should have a protocol in place for how to properly respond if faced with such an investigation.

Also, be sure to implement BA policies and procedures and effective agreements. Often, organizations don’t have BA agreements in place, or they have agreements that are not up to date, he said.

It’s an organization’s obligation to ensure it has a proper, written contract, Ginsberg said.

Another big problem is maintaining up-to-date, signed, and implemented policies and procedures. Be sure your policies and procedures are in sync with your current operations.

Date the changes to your policies and procedures. If you are audited by OCR, one of the first things it will ask for is copies of your current, written HIPAA policies and procedures, said Cone.

the same ownership or operational control as Shasta to attest to their understanding of permissible uses and disclosure of PHI, including disclosures to the media. The other facilities are located in California, Nevada, Pennsylvania, and Texas.

According to the resolution agreement, Shasta disclosed information about the patient on three occasions in December 2011. The initial disclosure involved a letter that was sent from Shasta’s parent company to a news outlet in response to a story about Medicare fraud. The letter described the patient’s medical treatment and provided specifics about her lab results.

Next, two of Shasta’s senior leaders met with a newspaper editor to discuss the patient’s medical record in detail. Finally, Shasta sent the Times a letter that included extensive information about the patient’s treatment. At the same time, Shasta sent an email to its entire workforce and medical staff (approximately 785–900 individuals) detailing the patient’s medical condition, diagnosis, and treatment.

Idaho State University case

The other resolution agreement reached this year was with Idaho State University (ISU), which settled a security case for $400,000. The settlement involved the breach of unsecured ePHI of 17,500 patients of ISU’s Pocatello Family Medicine Clinic, OCR said.

ISU agreed to pay $400,000 to settle alleged violations of the HIPAA Security Rule.

In August 2011, ISU notified HHS of the breach, which involved ePHI that was unsecured for at least 10 months as a result of disabled firewall protections at servers maintained by ISU. OCR subsequently launched an investigation revealing that the university’s risk analyses and assessments of its outpatient clinics were “incomplete and inadequately identified potential risks or vulnerabilities.” ISU also failed to assess the likelihood of potential risks occurring, OCR said.

ISU operates 29 outpatient clinics and is responsible for providing health information technology systems security at the facilities. Between four and eight of those clinics are covered entities subject to HIPAA rules, including the clinic where the breach occurred.

OCR concluded that ISU did not apply proper security measures and policies to address ePHI risks and did not have procedures in place for routine review of its information system, which could have detected the firewall breach much sooner.

“Risk analysis, ongoing risk management, and routine information system reviews are the cornerstones of an effective HIPAA security compliance program,” said OCR Director Leon Rodriguez in a press release.

ISU agreed to a two-year CAP to address the issues uncovered by the investigation.
The release of the HIPAA Omnibus Rule has left most HIPAA privacy and security officers with a long and likely overwhelming to-do list. “Buried is the operative word,” says one HIPAA privacy/security officer. “We’re on track with implementation, but it’s almost a 24/7 venture these days.”

The 563-page final rule released by HHS in January created an abundance of work for privacy and security officers. Their punch lists include activities ranging from revising the notice of privacy practices and updating HIPAA policies and procedures, to reviewing business associate (BA) contracts and modifying breach notification and response processes.

Healthcare organizations have until September 23 to comply with most of the provisions in the final rule.

Get others involved

While HIPAA privacy and security officers may be taking the lead on these initiatives, they do not have to go it alone, says Phyllis A. Patrick, MBA, FACHE, CHC, president of Phyllis A. Patrick & Associates, LLC, in Purchase, N.Y.

“A lot of people are saying they are feeling overwhelmed,” she says. However, resourceful HIPAA officers are dividing the workload, Patrick says.

Organizations should put forth a collaborative effort to implement all of their changes, agrees Frank Ruelas, MBA, principal of HIPAA College in Casa Grande, Ariz. It is crucial to draw others—from medical records staff to information technology (IT) leaders—into the process, he says.

How much work organizations have to do will depend on whether they made changes based on the interim HIPAA rules or waited until the final rule was released last January, Patrick says.

“I think it’s all over the ball park,” Patrick says, about where organizations stand when it comes to compliance. Those with dedicated HIPAA staff and the appropriate resources will be in better shape. Smaller organizations, or those whose HIPAA privacy and security officers wear multiple hats, may have more work ahead, she says.

The key is knowing what you need, says Ruelas, who compares the situation to a shopper going to the grocery store without checking what’s in the refrigerator and cabinets. If you haven’t done so, boil down the final rule to identify what’s new for your organization and put a plan of action in place, he said.

Create checklists for your departments

One way to divide the work is to create checklists for different departments, says Patrick. Review the changes brought about by the final rule and look at the different entities involved. What departments have a role to play? Consider involving HIM, IT, HR, legal, risk management, patient advocacy, and security.

Pull together leaders from your various departments to set up a workgroup, Patrick says. Hold a workshop to review what’s required by the final rule and what is new for your organization. The HIPAA privacy/security officer can take the lead in educating other department leaders on the changes they need to be aware of and the actions that need to be taken, she says.

For example, your legal department should be involved in updating your BA agreements based on the new requirements in the final rule. You should involve patient accounting in shaping your process to accommodate patients who, as allowed under the new rule, restrict disclosure of PHI to their health plan if they pay in full and out of pocket for a healthcare item or service.

Start with your policies that relate to privacy, security, and breach notification, and see how those relate to various departments, Patrick says. Several of these policies will relate to medical records, making the HIM department a critical link in your compliance efforts, she says.

Patrick’s associate Aviva M. Halpert, MA, RHIA, CHP, former chief HIPAA officer, has created a checklist for the HIM department. (See p. 8 for a copy of the checklist.) Organizations can adapt this checklist to meet the needs of their departments. Patrick plans to create more checklists and will post them on the company website at www.phyllispatrick.com.

As you create a checklist, ask what policies need updating. Have you modified key definitions—such as
Briefings on HIPAA

August 2013

those for marketing, fundraising, and subcontractors—to reflect the final rule? Have you updated forms to comply with the final rule? “It’s sort of a wheel,” Patrick says.

When you’ve made changes, your HR department can help bring them full circle and should be involved in the training of your workforce and implementing sanctions if the policies and procedures are not followed.

Bring in the right people

Don’t work in isolation, and don’t make the mistake of thinking only the department managers or directors can help you, Ruelas says. Other staff members may have great ideas.

“This is the time to capitalize on your mental Rolodex. If you have a question on ‘X’, get these people in a room and let them help you nail down your process,” he says. However, you may want to have a more informal workgroup and create an environment where staff members are comfortable sharing their ideas, he notes.

It’s also a good idea to check which departments contribute to your designated record set, he says. For instance, your laboratory or imaging department may have its own record system. However, when a patient requests his or her designated record set, you will need to provide not only a copy of an electronic health record but all of the patient’s data. If a department maintains any part of the patient record, bring them to the table, Ruelas says.

Prioritize your workload

If you have a long to-do list, you have to prioritize, says Patrick. “You know the areas of greatest weakness,” she says. If key policies are missing, put those in place. Address the major changes brought about under the final rule: your breach notification process and the requirements that govern BAs.

The old test-taking strategy of finishing the easiest questions first may not be a good strategy here, Ruelas says. Some of the more complicated items on your to-do list may take the longest to accomplish and you need to get started on them right away, he says. For instance, if you need an executive team to approve your new notice of privacy practices and it will take a month to get through that process, you need to plan for that.

“The key is to have a plan and to be moving in the right direction,” Patrick says. “It’s not going to help to throw up your hands.”

Ruelas agrees. “Have an open mind and keep it in context,” he says. The September 23 compliance deadline does not mean that OCR will be knocking on your door September 24 to check that you have brought everything up to date with the new rules. But if you were so unlucky as to be audited, OCR would want to know what you have done. “Start developing a track history. Show that you are making a genuine, professional effort. You want to have milestones,” he says.

Get support from leadership

Resourceful HIPAA officers are also winning over support from their organization’s leadership, Patrick says. Be sure you explain to leaders at the top of your organization what is involved. “This is a lot of work. It’s not just rewriting a couple of policies,” she says.

Have a dialog with your organization’s senior team. Show them the latest breach statistics from the OCR website so they understand how costly a breach can be, Patrick says.

Those leaders may be able to help you with the workload, Ruelas says. “Go to the powers that be and say, ‘Here’s what we need to do,’ ” he says.

There may be some room to adjust your workload and postpone or delegate lower-priority projects so you can work toward meeting the compliance deadline, he says.

It’s also a good idea to have an administration representative attend meetings, Ruelas says. When the message is clear that top leaders are committed to getting the compliance work done, other managers may be prompted to take action.

Don’t be afraid to reach out to colleagues at other organizations and see what solutions they have found. “We can learn from each other,” he says.

Re-focus on HIPAA

Now is also a good time to get people thinking about HIPAA, says Patrick. Think about making a push in September or early October to reintroduce privacy and security to your organization. “It’s an opportunity to get out there. Let people know there’s this new law and here’s what changed,” she says. This is a good time to enhance your program, develop more awareness, and build on your existing practices, Patrick says. ☛
HIM checklist for final rule preparation

✓ Do your existing HIM policies comply with the Omnibus Final Rule?
  • Do you have policies and procedures to comply with existing HIPAA requirements?
    – Accounting of disclosures
    – Confidentiality
    – Designated record set
    – Patient access
    – Right to amend medical record
    – Right to request confidential communication
  • Have you modified existing policies to comply with final rule changes?
    – Change in authorization requirements for records of deceased patients, immunization records
    – Change in authorization requirements for research
    – Minimum necessary
    – Patient right to electronic copy of electronic medical record
    – Use and disclosure of PHI
  • Have you created new policies to comply with new requirements in the final rule?
    – Right to restrict disclosure of records to third-party payers if they relate to encounters paid for out of pocket by the patient

✓ Do your existing forms comply with the final rule?
  • Do you have the forms necessary to comply with existing HIPAA requirements?
    – Authorization to disclose PHI
    – Authorization to disclose psychotherapy notes
    – Patient access request
    – Request to amend medical record
    – Request to rescind authorization
  • Have you modified existing forms to comply with the changes in the final rule?
    – Request to amend electronic medical record
    – Authorization for marketing
  • Have you created new forms to comply with new requirements in the final rule?
    – Request to receive copy of record in requested electronic format
    – Request to restrict disclosure of PHI relating to encounters paid for out of pocket to third-party payer

✓ Do you have complete and up-to-date versions of institutional policies and procedures regarding HIPAA/HITECH/final rule compliance that pertain to your department?
  • Access to PHI for research
  • Business associates (BA)
  • Enforcement
  • Health information exchanges
  • Incidental disclosure
  • Notice of privacy practices (NOPP)
  • Notification of breach
  • Role-based access
  • Sale of PHI
  • Sanctions
  • Training

✓ List of key definitions
  • Does your list include common current terms?
    – Accountable care organization
    – E-prescribing gateway
    – Health information exchange
    – Patient safety organization
    – Personal health record
    – Subcontractor
  • Have you modified your definition of terms to comply with changes in the final rule?
    – Breach
    – BA
    – Electronic media/electronic storage material
    – Fundraising
    – Health information organization
    – Marketing
    – PHI

✓ Do you have complete and up-to-date versions of forms relating to institutional policies and
procedures regarding HIPAA/HITECH/final rule compliance that pertain to your department?

• BA agreement (BAA)
• Code of conduct
• Employee security attestation/affirmation
• NOPP
• Acknowledgement of receipt of NOPP
• Patient bill of rights (applicable in New York state)
• Request for confidential communication
• Request to opt out of fundraising

✓ Do you provide annual HIPAA refresher training targeting HIM employees?

• Are employees required to complete training prior to being given system access?
• Are employees required to sign a form attesting to their understanding of all privacy and security policies prior to being given system access?

✓ HIM BAs

• Do you have access to a centralized database of BAAs?
• Do you have a complete list of your BAs?
• Do you/the organization have a BAA with each of your BAs?
• Have you created a plan to prioritize revisions to those BAAs that need revisions prior to the compliance dates (either 9/23/13 or 9/23/14)? Is it based on risk?

✓ Physical security

• Have you assessed the physical security of HIM and removed risks such as?
  – Combination to locked cabinet taped to wall
  – Key stored in obvious location accessible by anyone

  • PHI/confidential files left on desktop or in unlocked drawers after hours
  • Security cameras turned off and/or not monitored
  • Unlocked door to unattended department

✓ Workstation security

• Do all HIM workstations comply with institutional policies for security?
• Is data on all portable devices/drives encrypted?
• Is data on portable devices backed up?
• Are passwords secure and not posted on or near workstation?
• Is the timeout set to standard?

✓ Access control and practices

• Do you have a list of access rights necessary for each HIM job function? For each position?
• Do you comply with institutional standards for access controls?
• Are employees provided with the minimum access necessary to perform their jobs?
• Is notification of a user’s termination provided to access management in a timely fashion?
• Are access rights reassessed and revised if necessary when a user transfers to a new position?
• Do you have a policy for providing temporary access rights to regulatory or other authorized outside reviewers?
• Do you have a list of temporary access codes that can be assigned as needed?
• Do you ensure that temporary codes are not reused?
• Do you track who was assigned to each temporary code and when?

References

HIPAA Privacy and Security: 45 CFR 164 Subpart E
Final Omnibus Rule: 78 FR 5565-5702, 45 CFR 160, 164

Address enhanced individual rights to comply with the final rule

Editor’s note: The following is adapted from the HCPro book The HIPAA Omnibus Rule: A Compliance Guide for Covered Entities and Business Associates, by Kate Borten, CISSP, CISM, president of The Marblehead Group in Marblehead, Mass. To learn more about the book, go to www.hcmarketplace.com.

The HIPAA Omnibus Rule amends the Privacy Rule to strengthen individuals’ right of access to and control of their PHI.

PHI disclosure restrictions for out-of-pocket payments

The Omnibus Rule expands 45 CFR 164.522 [Rights to request privacy protection for protected health information] by adding a new right at 45 CFR 164.522 (a)(1)(vi):

A covered entity must agree to the request of an individual to restrict disclosure of protected health information about the individual to a health plan if:

(A) The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and

(B) The protected health information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full.

This is a powerful privacy right that has existed informally in years past before automated record and billing systems became common. The rule writers acknowledge its importance by requiring covered providers to amend their privacy notices to include it explicitly. However, today’s interconnected electronic systems and payment processes can make compliance with these restriction requests challenging and complex.

The Omnibus Rule preamble addresses an important exception—disclosures required by law. If state or other law requires a covered provider to submit claims and no exception or opportunity for individuals to pay out of pocket exists, the covered entity (CE) may not grant the request. Medicare Conditions of Participation are considered required by law, implying that disclosure of PHI may be necessary (e.g., audits). However, if a beneficiary or legal representative refuses to sign a CE’s form authorizing claim submission, the CE can grant the individual’s request and not submit the claim.

The practice of bundling services for billing purposes can be problematic with respect to this right. For example, a patient who sees a provider for two unrelated conditions requests a restriction on a portion of the encounter and wants to pay out of pocket for that portion only. The rule should apply and require the covered provider to grant the request. However, services sometimes do not separate cleanly. In this scenario, a provider should advise the individual that the health plan may be able to infer information about the condition and services which were paid out of pocket. Furthermore, when services cannot be unbundled, the provider should inform the individual and offer the opportunity to pay out of pocket for the entire bundle.

The Omnibus Rule clarifies that individuals are responsible for requesting similar restrictions by other healthcare providers, such as pharmacies and laboratories. However, automated systems and gateways that instantly transmit orders from a physician’s office to a laboratory or pharmacy, for example, can be problematic with respect to this right. For example, an e-prescribing system can transmit a prescription that a pharmacy fills and for which it generates a claim before the individual has an opportunity to request the restriction at the pharmacy. In this scenario, covered providers (e.g., the physician office) should counsel the individual and make reasonable efforts to assist in achieving the privacy goal. For example, some providers could offer paper prescriptions when an individual requests this restriction.

Note that some HMOs may not permit claim withholding. In this case, the Omnibus Rule preamble suggests that providers counsel individuals to go out of network for the service. A provider that can treat a patient on an out-of-network basis should do so to comply with the restriction. Further, rule writers suggest that HMO contracts be modified to avoid the problem. The preamble states:
We would not consider a contractual requirement to submit a claim or otherwise disclose protected health information to an HMO to exempt the provider from his or her obligations under this provision. Further, the final rule provides a 180-day compliance period beyond the effective date of these revisions to the Privacy Rule, during which provider contracts with HMOs can be updated as needed to be consistent with these new requirements.

Providers should be prepared to respond in situations involving dishonored payments (e.g., individual’s check returned for insufficient funds). Providers are expected to make reasonable efforts to obtain payment (e.g., alternative form of payment) before submitting a claim. The rule allows providers to require full payment when restriction is requested and before the service is provided.

Note that providers may not be able to implement restrictions when individuals request them after care has begun (e.g., during a hospital stay).

Individuals who receive follow-up care for prior services that are subject to a disclosure restriction must request restriction again if they intend continued disclosure restriction with respect to the follow-up care. Providers should discuss this with individuals during follow-up care to make them aware of the potential disclosure and offer an opportunity to request restriction and pay out of pocket. Otherwise, providers may submit claims, even if doing so reveals PHI that pertains to the prior restricted service.

The preamble states that individuals may pay out of pocket with funds from a flexible spending account (FSA) or health savings account (HSA), but PHI may not be restricted from disclosure to the FSA or HSA when making a payment.

(See the box on p. 12 for the compliance steps healthcare organizations should take.)

Individuals’ requests for copies of PHI

The HIPAA Privacy Rule at 45 CFR 164.524 [Access of individuals to PHI] grants individuals a right to view and receive a copy of their own PHI in CEs’ designated record sets. Note that CEs are required to document what their designated record sets comprise. BAs sometimes maintain source data in a designated record set on behalf of CEs.

The Omnibus Rule strengthens the right of access in several ways. First, 45 CFR 164.524(c)(2)(ii) requires that CEs (and BAs acting on behalf of CEs) must do the following when individuals request electronic copies of their PHI in designated record sets, and PHI is maintained electronically:

[They] must provide the individual with access to the protected health information in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the covered entity and the individual.

The 10-year old Privacy Rule required only that CEs provide an electronic copy if the PHI was readily producible in the electronic format requested. Now CEs must produce the PHI in some common format. This expanded right does not necessarily mean that affected CEs or their BAs must purchase new systems or provide PHI in a specific format to ensure compliance. However, ePHI, including linked images, must be producible in some common format for individuals who request it.

The second notable enhancement is 45 CFR 164.524(c)(3)(ii), which states:

If an individual’s request for access directs the covered entity to transmit the copy of protected health information directly to another person designated by the individual, the covered entity must provide the copy to the person designated by the individual. The individual’s request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of protected health information.

This makes explicit the intent of the original Privacy Rule to require CEs to transmit PHI copies upon the request of an individual. This applies regardless of whether PHI is in electronic, paper, or other format.

This differs from provisions that govern other similar individual rights, however. This provision requires that this type of request be in writing (paper or electronic format) with details and include an actual or electronic signature to avoid misunderstanding that could lead to a breach.

Combining this request with other forms (e.g., an individual’s request for a personal copy of PHI)
permissible. However, the Omnibus Rule preamble states that this is not a HIPAA authorization form that requires more information than necessary to exercise this right.

The original Privacy Rule requires responding to access requests within 30 days, but it allows an extension when targeted PHI is not maintained or accessible on-site. The Omnibus Rule reduces the extension from 60 to 30 days at 45 CFR 164.524(b)(2)(ii).

The original Privacy Rule permits CEs to charge reasonable cost-based fees for copying PHI. The rule at 45 CFR 164.524(c)(4)(i) separately identifies labor costs, 45 CFR 164.524(c)(4)(ii) separately identifies the cost of supplies for creating paper or electronic copies, and 45 CFR 164.524(c)(4)(iii) identifies the cost of postage.

### Compliance steps for PHI disclosure restrictions for out-of-pocket payments

The following compliance steps apply to covered entities (CE) that are healthcare providers. Business associates (BA) that perform these activities on behalf of CEs are contractually liable.

Health plans with provider contracts that conflict with this right should review contract language and revise it to conform with the new rule.

1. **Document**
   Organizations should already have policies that acknowledge and commit to honoring a patient’s right to request certain restrictions on PHI use and disclosure, as required by the Privacy Rule. They should revise their policies to acknowledge and commit to this new individual right to request restrictions.

2. **Review**
   Work with your organization’s providers, registration, patient financial services, billing specialists, and information technology staff to identify scenarios in which patients are likely to request disclosure restrictions and scenarios in which staff should initiate conversations about restriction (e.g., follow-up care).

   Identify any laws or regulations that require PHI disclosure and conflict with this right. Document them and the particular circumstances. Identify any health plan contracts that require PHI disclosure that conflicts with this right.

   Review how your organization currently discloses PHI to health plans (and their BAs, if relevant) for payment and healthcare operations (i.e., via which systems and triggered by which events) and then determine whether the systems have the ability to restrict disclosure on an on-demand basis (e.g., change the encounter to self-pay).

   Consider the problems discussed previously (i.e., bundling, e-prescribing gateways, follow-up encounters, dishonored payment) and how they apply to your organization’s processes, workflow, computer systems, and other factors.

3. **Develop**
   Develop, test, document, and implement solutions for your organization. These may include policies, procedures, scripts, and technology.

   Develop and document procedures for responding to restriction requests and for addressing the problems noted previously. Develop patient counseling scripts.

   If appropriate, work with health plans to modify contract language to facilitate compliance with this rule.

   If system solutions are lacking, compare the cost of technical changes and manual procedures, if any. Develop and document manual procedures as needed.

4. **Train**
   Ensure that all workforce members are aware of this new patient right. Further, identify clinical and support staff whose responsibilities will include a role in receiving and implementing restriction requests in your organization. Provide training that explains these responsibilities. Ensure that relevant policies, procedures, and other resources (e.g., internal hotline for requesting assistance) are readily available to them.

Source: Adapted from the book The HIPAA Omnibus Rule: A Compliance Guide for Covered Entities and Business Associates, by Kate Borten, CISSP, CISM, president of The Marblehead Group. Published by HCPro, Inc.
Tips from this month’s issue

Common deficiencies targeted in OCR corrective action plans (p. 1)

1. When conducting a risk analysis within your organization, be sure to thoroughly document what you have done. Going through a simple checklist is not a risk analysis and does not provide sufficient documentation.

2. Business associates (BA) are now subject to the HIPAA security rule and must conduct a risk analysis. Plan accordingly.

3. Lack of training prior to allowing staff to access PHI is a common problem for many organizations.

4. A standard “HIPAA 101” training program won’t cut it. Be sure to sufficiently customize training to your organization’s actual practices.

5. Remember to provide initial training and follow-up training to all members of your workforce.

6. Train your workforce on security awareness and provide periodic reminders.

7. If your organization adopted policies and procedures years ago from purchased templates, now is a good time to update them based on current business practices.

8. Be on the lookout for safeguards and controls for mobile devices when you evaluate the security risks for your organization.

9. Devise and implement a “bring your own device” policy that will help to safeguard PHI.

10. Establish and enforce sanctions for dealing with workforce members who violate HIPAA policies and procedures.

11. Log security incidents and document what you have done to mitigate problems.

12. Maintain up-to-date, signed, and implemented policies and procedures that are in sync with your current operations. Date the changes to these policies and procedures.

Divide (the workload) and conquer (p. 6)

13. Review the final rule and determine what parts apply to your organization.

14. To comply with the final rule, create a punch list of activities ranging from revising the notice of privacy practices and updating HIPAA policies and procedures, to reviewing BA contracts and modifying breach notification and response processes.

15. Divide the workload. Organizations should put forth a collaborative effort to implement all of the final rule changes.

16. Pull together leaders from your various departments to set up a workgroup.

17. The HIPAA privacy/security officer should take the lead in educating other department leaders on the changes they need to be aware of and the actions that need to be taken.
18. Your legal department should be involved in updating your BA agreements based on the new requirements in the final rule.
19. Develop checklists for different departments to determine which policies need updating.
20. Don’t work in isolation or think only the department managers or directors can help you. Other staff members who work “in the trenches” may have great ideas.
21. If you have a long to-do list, you have to prioritize. Some of the more complicated items on your to-do list may take the longest to accomplish, so you need to get started on them right away.
22. Have a dialog with your organization’s senior team. Show them the latest breach statistics from the OCR website so they understand the cost of a breach.
23. Have an administration representative attend meetings. This could prompt other managers to take action when the message is clear that top leaders are committed to getting the work done to be sure you are in compliance.
24. Don’t be afraid to reach out to colleagues at other organizations and see what solutions they have found.

Address enhanced individual rights to comply with the final rule (p. 10)
25. If state or other law requires a covered provider to submit claims and no exception or opportunity for individuals to pay out of pocket exists, the covered entity (CE) may not grant the request.
26. If a beneficiary or legal representative refuses to sign a CE’s form authorizing claim submission, the CE can grant the individual’s request and not submit the claim.
27. When services cannot be unbundled, the provider should inform the individual and offer the opportunity to pay out of pocket for the entire bundle.
28. Some HMOs may not permit claim withholding. In this case, the Omnibus Rule preamble suggests that providers counsel individuals to go out of network for the service.
29. Be prepared to respond in situations involving dishonored payments and make reasonable efforts to obtain payment before submitting a claim.
30. Don’t forget that CEs are required to document what their designated record sets comprise.
31. Make sure you have a means of producing ePHI, including linked images, in some common format.