HHS releases HIPAA Omnibus Rule

Finally ... it’s final

Unless you’ve been completely out of touch, by now you know that HHS has finally released the final rule that HIPAA privacy and security officers have been waiting for.

On January 17, HHS released the 563-page “Omnibus Rule,” which is also being called the HIPAA mega rule and HIPAA 2.0, that modified the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules.


The final rule implements most of the privacy and security provisions of HITECH and extends the reach of HIPAA. With a few exceptions, organizations must comply with the final rule by September 23—180 days after publication.

In a nutshell, the new rule:

• Modifies the breach notification standard

Number of pages in HHS’ new HIPAA Omnibus Rule, released January 25.

Number of days after publication of the HIPAA final rule that organizations have to comply with it.

Organizations must notify HHS of breaches affecting fewer than 500 individuals within 60 days of the end of the calendar year in which the breach was discovered.

SOURCE: HHS.
Quick Hits

Report: Lost documents, portable memory devices to blame for majority of data breaches

Lost paper files and portable memory devices account for 65% of data breaches according to a survey conducted by the Society of Corporate Compliance and Ethics and the Health Care Compliance Association.

The compliance and ethics department, according to 69% of respondents, led the remediation effort following the last data breach.

http://blogs.hcpro.com/hipaa

FTC issues privacy recommendations for mobile devices

The Federal Trade Commission (FTC) issued a report in February recommending privacy safeguards for mobile devices.

The report, Mobile Privacy Disclosures: Building Trust Through Transparency, says mobile devices raise a number of potential privacy risks.

http://blogs.hcpro.com/hipaa

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.
• Expands certain HIPAA provisions to business associates (BA) and their subcontractors
• Expands patient rights to access their PHI and to restrict its disclosure
• Imposes new rules on the use and disclosure of PHI
• Strengthens the government’s ability to enforce HIPAA
• Addresses obligations under the Genetic Information Nondiscrimination Act of 2008 (GINA)

A daunting first look

The almost 3-inch thick final rule is a bit daunting. But remember, much of it will be familiar from the previously published interim final rule. “There were not too many big surprises,” says Adam H. Greene, JD, MPH, a partner in Davis Wright Tremaine, LLP’s Washington, D.C., office. A former OCR regulator, Greene was involved in the rulemaking process when he worked at the agency.

The final rule remains fairly consistent with the proposed rule released in July 2010, but there are some significant differences.

How much work you have to do to get into compliance will depend on the state of your existing HIPAA privacy and security program. “People should be in decent shape from the standpoint that there were not a lot of surprises,” Greene says. “But HIPAA compliance efforts have always been fighting for resources and the reality is many people had a long way to go [to comply]. This just adds to that challenge.”

So get familiar with the final rule. “The bottom line is we have lots of reading to do,” says Frank Ruelas, MBA, principal of HIPAA College in Casa Grande, Ariz.

Although you may have been able to avoid reading Moby Dick in your high school English class and pass the test by reading the CliffsNotes version, that’s not recommended here, says Ruelas. “You’re going to need to be very familiar with Captain Ahab,” he says, referring to the book’s villain.

Bite the bullet, and delve into the final rule, he says. If you are responsible for HIPAA compliance, it’s your job. “People owe it to themselves, their organization, and their patients to go through the regulations,” he says.

It’s worth your time to not just read the rule itself, but to look at the preamble as it contains a lot of insight and detail, says Elizabeth H. Johnson, Esq., a partner at Poyner Spruill, LLP.

Some of the big changes

Although some provisions haven’t changed, the final rule makes some changes that will impact covered entities (CE), BAs, and their subcontractors. Let’s look at some of the significant changes:

• Breach notification. HHS has eliminated the “harm threshold” provision from the Breach Notification Rule. Under that provision, CEs were only required to provide notice of a security breach if it posed a significant risk of harm to the affected individuals. Under the final rule, any use or disclosure of PHI that is not permitted by the Privacy Rule will be presumed to be a reportable breach. CEs and BAs will need to conduct a risk analysis using factors set by HHS. “But the agency has made clear its expectation that impermissible uses and disclosures of readily accessible PHI will likely be a reportable breach,” says Johnson. The change will mean an increase in the number of breaches organizations will need to report, Johnson and Greene predict. (For more on breach notification, see the story on p. 8.)

• Stiffer requirements for BAs and subcontractors. HIPAA has become a fact of life for BAs and their subcontractors who use and disclose PHI. Much of the Privacy Rule and all of the Security Rule now apply directly to both. So BAs and subcontractors will need to create and implement a HIPAA compliance plan if they don’t have one in place already.

• New limits on uses and disclosures of PHI. The final rule addresses a number of privacy issues related to the uses and disclosures of PHI, such as communications for marketing or fundraising, exchanging PHI for remuneration, disclosures of PHI to persons involved in a patient’s care or payment for care, and disclosures of student immunization records, says Johnson.

There was good news and bad for healthcare organizations. One pleasant surprise for the industry was the expansion of the use and disclosure of PHI
for fundraising purposes, says Greene. Previously, an organization could use or disclose only demographic information and dates of service for fundraising.

Now HHS expanded the categories of PHI that may be used and disclosed for fundraising to also include:

- Department of service
- Treating physician
- Outcome information
- Health insurance

For instance, a hospital that wants to raise money for a new cancer center can target individuals served by its oncology department who had a positive outcome based on treatment, says Greene.

Another piece of good news was a change that affects clinical research. The final rule allows a blending of “conditioned” and “unconditioned” authorizations into a single document.

The bottom line for those conducting research is that it simplifies authorization paperwork.

The bad news for CEs is more restrictions on marketing and sale of PHI, says Greene. The final rule expands what uses and disclosures of PHI are considered marketing and require an individual’s authorization.

- **Expanded focus on patient rights.** The final rule expands an individual’s rights to access electronically stored PHI. Organizations are required to give patients their medical record in the form and format requested, if readily producible. If it is maintained electronically, then CEs must provide patients an electronic copy.

An individual may designate a third party to receive the copy of his or her PHI. The request must be in writing, clearly identify the designated person, and clearly identify where to send the copy.

- **Restriction for out-of-pocket payments.** The final rule also allows patients to restrict information for out-of-pocket payments. CEs must agree to an individual’s request to restrict disclosure of PHI to a health plan if the healthcare item or service has been paid out of pocket and in full, unless the disclosure is required by law. This applies if an individual or person on the individual’s behalf pays for the item or service.

This is probably the most challenging change for healthcare organizations to comply with from an operational viewpoint, says Greene.

“It sounds easy in theory. In practice, it is difficult to segregate data in this fashion,” he says. “Segregating the information is not necessarily supported by current technology and process. People are dumbfounded on how to operationalize that.”

His advice to clients? “Do their best. Put forth a good-faith effort. Try to segregate the information,” he says. For instance, organizations might put automatic “pop-ups” in the medical records when there is a restriction in place to indicate that not all information in the medical record should be shared. Healthcare organizations should also keep the issue in mind if audited by a health plan, since there may be patient information that should not be disclosed to the health plan.

- **Notice of Privacy Practices.** The final rule changes the requirements for what organizations must include in their Notice of Privacy Practices.

Updated notices must advise individuals of required changes in the rule, including:

- The prohibition on the sale of PHI without the written authorization of an individual
- The duty of the CE to notify affected individuals of a breach of unsecured PHI
- The individual’s right to opt out of receiving fundraising communications
- The right to restrict disclosure to a health plan when the patient pays out of pocket

For example, organizations will need to address a breach notification in that notice, says Rebecca L. Williams, JD, RN, a partner in Davis Wright Tremaine, LLP’s Seattle office.

The final rule makes it clear that genetic information is included in the definition of “health information” and is subject to HIPAA rules if it is individually identifiable. Under GINA, healthcare plans are prohibited from using and disclosing genetic information for underwriting purposes.

- **Increased enforcement.** BAs and their subcontractors are now subject to civil money penalties and other enforcement actions for noncompliance with applicable provisions of HIPAA, says Greene.

Under the final rule, OCR will investigate all cases of possible willful neglect, he says.

Willful neglect is defined as a “conscious, intentional failure or reckless indifference” to the obligation to comply with HIPAA. OCR will impose a penalty for all violations of willful neglect.
An important fact that’s been missed by many people is that HHS has clarified that the enforcement provisions are not new or modified standards or implementation specifications, says Chris Apgar, CISSP, CEO and president of Apgar & Associates, LLC, in Portland, Ore.

That means that the enforcement provisions are effective when the rule is effective—on March 26, rather than September 23 when the compliance date kicks in, he says. Based on the language in the final rule and the preamble, OCR could levy civil penalties retroactively to February 18, 2009, when those provisions became statutory reality with the HITECH Act.

It appears BAs’ liability would start February 18, 2010, the statutory compliance date for BAs, Apgar says.

An important fact that’s been missed by many people is that HHS has clarified that the enforcement provisions are not new or modified standards or implementation specifications, says Chris Apgar, CISSP, CEO and president of Apgar & Associates, LLC, in Portland, Ore.

That means that the enforcement provisions are effective when the rule is effective—on March 26, rather than September 23 when the compliance date kicks in, he says. Based on the language in the final rule and the preamble, OCR could levy civil penalties retroactively to February 18, 2009, when those provisions became statutory reality with the HITECH Act.

It appears BAs’ liability would start February 18, 2010, the statutory compliance date for BAs, Apgar says.

Ten steps to help you comply with the HIPAA final rule

Privacy and security officers got their marching orders when HHS released the long-awaited new HIPAA “Omnibus Rule” in January.

To comply with the final rule, healthcare organizations need to get working on a number of activities. The rule is enforceable 180 days from its publication in the Federal Register January 25, giving organizations until September 23 to get into compliance.

Each healthcare organization will need to determine where its priorities lie, depending on its current HIPAA compliance program.

“There’s work here for probably everyone,” says Phyllis A. Patrick, MBA, FACHE, CHC, president of Phyllis A. Patrick & Associates, LLC, in Purchase, N.Y. “But this is not all new if you have a compliance program. Take it in steps. I think it is all doable.”

So where can you get started with the 563-page final rule? HIPAA consultants and attorneys advised taking the following 10 steps:

1. Conduct a risk analysis. You’ve heard it many times before, but a risk analysis is a good starting place, says Chris Apgar, CISSP, CEO and president of Apgar & Associates, LLC, in Portland, Ore. By conducting a risk analysis, you will determine what specific risks your organization faces. From there, you can create your own list of actions you need to take and set priorities. With a risk analysis, you will find out whether you are missing a particular policy or need to update a certain procedure.

Make sure your risk analysis reflects vulnerabilities highlighted in recent HHS guidance, such as the threat to the security of PHI from mobile devices, says Adam H. Greene, JD, MPH, a partner in Davis Wright Tremaine, LLP’s Washington, D.C., office. “HHS has made clear the risk assessment is a high priority,” he says.

2. Amend your Notice of Privacy Practices. Some organizations may not have looked at this for years or delayed updating their notice until HHS published the final rule, says Frank Ruelas, MBA, principal of HIPAA College in Casa Grande, Ariz.

Review your existing Notice of Privacy Practices and be sure you address the additional patients’ rights included in the final rule. It’s a good springboard to begin to address all the actions you must take, says Ruelas. For instance, under the final rule a patient has the right to direct an organization to transmit his or her PHI electronically to a third party. That gives rise to a review of policies and procedures and draws others, such as your medical records and information technology leaders, into the process. That collaborative effort can build momentum as you implement all of the final rule changes, he says.

Once it’s revised, make sure the new Notice of Privacy Practices is properly posted and distributed. You will need to provide it to new patients and make the revised notice available to existing patients, Ruelas says.

It’s also a good idea to distribute and discuss the Notice of Privacy Practices with your workforce members, says Patrick. “It’s really the contract your organization has with the patient.”
**Briefings on HIPAA**

3. **Review and update your privacy and security policies and procedures.** Read the rule and perform a gap analysis to determine what policies and procedures you need to revisit in light of the changes, says Greene. For instance, you may need to make changes based on new marketing restrictions and restrictions on disclosures of PHI, he says.

This is also a good opportunity to review and update your existing policies and take into account OCR guidance, he says. The agency recently released guidance on de-identification and mobile devices.

It’s also a good time to fine-tune policies based on your experience, says Rebecca L. Williams, JD, RN, a partner in Davis Wright Tremaine, LLP’s Seattle office. Look at what has worked and what has not in your organization.

4. **Revise your breach notification policies, procedures, and breach response plans.** This is critical in terms of how you conduct a risk assessment to determine whether breach notification is required. Under the final rule, the “harm threshold” is gone and you must now determine whether unsecured PHI was “compromised.” (See story on p. 8.)

Modify your breach response process and then be prepared to perform that risk analysis quickly and continuously, says Elizabeth H. Johnson, Esq., a partner at Poyner Spruill, LLP. Each time you have a breach, you must go through the risk assessment process to determine whether there was a low probability PHI was comprised. Include the four factors identified in the final rule in your analysis, says Patrick. To reduce reportable breaches, take advantage of the safe harbor provisions by encrypting PHI according to HHS guidance, says Greene.

5. **Revise your business associate (BA) contract templates and begin the process of amending and negotiating each one.** This is a big job, says Johnson. Even if you looked at those BA agreements in light of the interim final rule, take another look, she says. Be sure your BA agreements address time frames that ensure you will be notified quickly of a possible breach. In light of new breach notification requirements and increasing compliance reviews, consider appropriate liability protections and indemnification in your BA agreements, she says.

6. **If you are a BA or subcontractor, get started now with your HIPAA compliance efforts.** Ramp up your efforts to comply with the provisions of the final rule, says Johnson. You are now directly responsible for protecting PHI under the rule. You have until September to fully comply with the HIPAA Security Rule and provisions of the Privacy Rule.

Now the stakes are much higher for not complying, says Greene, including enforcement action from OCR.

7. **Take a look at your organization in light of new limits on uses and disclosures of PHI.** Review the communications you are sending to patients, says Johnson. Be sure your communications with patients conform to new requirements for marketing and fundraising included in the final rule, she says.

Don’t forget to update your forms, such as those for requests for access, if necessary, says Williams.

8. **Be aware of increased patient rights.** One major change is the requirement to provide patients with electronic copies of their medical records. Develop a strategy for providing copies of electronic records, says Patrick. For instance, you may have a decentralized process. Some information may be documented in the radiology department. Other test results may reside in your laboratory. How do you bring all the pieces together? Patrick says healthcare organizations are asking how they should document requests for electronic records and how they should charge the patients.

9. **Train your workforce on all the changes that result from the final rule.** For instance, make workforce members aware of changes to your Notice of Privacy Practices. Retrain workforce members on breach notification, as well as marketing and fundraising rules, says Johnson. Workforce members may also need updating on just who is a BA. Be sure your staff members know what are impermissible uses and disclosures, says Ruelas. Be sure they know what to look for and what to report as a possible breach.

10. **Adopt what OCR calls a “culture of compliance.”** Reintroduce privacy and security, says Patrick. You may want your CEO to draft a memo or email letting those in your organization know about the final rule changes and the need to reestablish efforts to protect PHI, she says. Part of your culture of compliance is verifying and reinforcing sanctions so there are consequences for violating your HIPAA policies and procedures, says Greene.
HIPAA becomes reality for BAs, subcontractors

HIPAA has hit home for business associates (BA) and their subcontractors.

The release of the final HIPAA Omnibus Rule will have a major impact on BAs and subcontractors, as well as the covered entities (CE) that are the first rung in the ladder of HIPAA responsibility.

With the final rule, responsibility to protect PHI now rests on BAs and their subcontractors. Many of the provisions of the Privacy Rule and all of the Security Rule now apply directly to both. BAs now have direct liability under the Omnibus Rule for impermissible use and disclosures of PHI and must notify CEs of a breach.

Those who don’t have a HIPAA compliance plan in place have lots of work to do before September 23, the deadline for compliance with the final rule.

A new crop of BAs

In fact, the final rule has provided a new, broader definition of BAs. A BA is, and continues to be, an entity that performs functions, activities, or services on behalf of CEs that involve use or disclosure of PHI.

However, HHS has modified the rules to provide that BAs may “create, receive, maintain, or transmit” PHI on behalf of a CE. That means there is “a whole new crop of BAs,” says Rebecca L. Williams, JD, RN, a partner in Davis Wright Tremaine, LLP’s Seattle office.

The new definition clarifies that entities that merely store PHI are also BAs, says Elizabeth H. Johnson, Esq., a partner at Poyner Spruill, LLP.

The lack of a contract between a CE and BA will not prevent the designation, she says.

HHS has clarified that organizations providing personal health records on behalf of CEs are BAs. Health Information Organizations, including health information exchange organizations, e-prescribing gateways, and other entities that transmit PHI on behalf of CEs, are BAs if they access PHI on a “routine basis,” says Johnson.

Although some BAs may have argued with CEs in the past that they weren’t BAs, the guidance provided in the rule’s preamble clarifies their status. Records storage services, shredding companies, and cloud service providers are all BAs.

On the other hand, some organizations have included all kinds of contractors on their list of BAs, says Phyllis A. Patrick, MBA, FACHE, CHC, president of Phyllis A. Patrick & Associates, LLC, in Purchase, N.Y. “Take those that aren’t BAs off your list if they don’t deal with PHI,” she says.

Subcontractors in the mix

Under the final rule, subcontractors of BAs are, by definition, now themselves considered BAs if they create, receive, maintain, or transmit PHI, says Johnson.

“Welcome to the HIPAA party,” says Williams.

You can think of it like a ladder, with the subcontractors of subcontractors having HIPAA responsibilities if they touch PHI. HIPAA responsibility is delegated down the line, Williams says.

BAs and their subcontractors have a short window of time to become compliant with the final rule.

The fallout for CEs

Given that CEs can be held liable for their BA’s noncompliance, organizations need to pay attention to those BA compliance efforts. That may include increased diligence, security reviews, and full-blown audits by CEs, says Johnson.

CEs are still required to contract with their BAs, but are not required to contract directly with their BAs’ subcontractors, says Johnson.

CEs should review all of their existing BA agreements, even if they have already made updates in anticipation of the rule changes, she says. You want to capture the provisions HHS is now mandating and modify contracts to cover those, she says.

Many, if not most, BA agreements are going to need to be amended, says Williams.

There is one exemption to the compliance deadline that applies to BA and data use agreements that existed prior to January 25, 2013. CEs do not need to update those existing agreements until September 22, 2014, with one provision—that they are not modified or renewed prior to that date, Johnson says. However, if you
Briefings on HIPAA

change or renew those BA agreements, then you must update them to comply with the final rule.

OCR has published sample BA agreement provisions on its website at www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html. However, Williams urges organizations to use the sample with caution.

“Don’t use it verbatim,” she says. It can provide you with some questions you should ask in preparing your BA agreements.

‘Harm threshold’ eliminated

Breach notification rules change

One of the biggest changes in the Omnibus final rule is in the way healthcare organizations will determine whether they need to notify affected individuals of a security breach.

The change is going to make breach notification more likely, says Adam H. Greene, JD, MPH, a partner in Davis Wright Tremaine, LLP’s Washington, D.C., office. Under the final rule, HHS eliminated the controversial “harm threshold” that required the reporting of a breach if there was a significant risk of financial, reputational, or other harm to affected individuals. Under that provision, if organizations could demonstrate there was no significant risk of harm, the incident was not a reportable breach and notice was not required.

Some members of Congress, as well as some consumer rights groups, argued against the harm threshold, saying it gave organizations too much leeway in deciding whether individuals should be notified of a breach of their PHI.

Low probability of compromise

The final rule amends the definition of a breach so that the impermissible acquisition, access, use, or disclosure of PHI is presumed to be a breach—and breach notification is necessary—unless a covered entity (CE) or business associate (BA) can demonstrate, through a documented risk assessment, that there is a low probability that the PHI has been compromised.

One way to remember it: “I call it low-pro-co,” says Frank Ruelas, MBA, principal of HIPAA College in Casa Grande, Ariz.

So it’s no longer the likelihood that affected individuals might be harmed, but the risk that PHI has been “compromised” that organizations must determine. It’s a presumed breach, unless a risk analysis reveals a low probability that PHI was compromised.

To determine whether there’s a low probability that PHI was compromised, the final rule identifies four factors that organizations must consider in their risk assessment:

• The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification (Did it include Social Security numbers, credit card numbers, or dates of birth? Did it include detailed or sensitive clinical information?)

• The unauthorized person who used the PHI or to whom the disclosure was made (Was the recipient another CE required to comply with HIPAA? Or could information have fallen into the hands of identity thieves?)

• Whether the PHI actually was acquired or viewed (Was PHI sent to a wrong address but envelopes were returned unopened? Or did an individual let you know he or she opened a letter that contained someone’s information?)

• The extent to which the risk to the PHI has been mitigated (Did you get an assurance from an employee, a BA, or other CE that he or she will not disclose the PHI?)

HHS says the “compromise” standard will result in a more objective evaluation of the risk to PHI. You can find further guidance on how to apply these four factors in the rule’s preamble. Organizations can consider
other factors as well in evaluating the overall probability that an incident compromised PHI.

As an example, the final rule describes a scenario where a CE misdirects a fax containing PHI to the wrong physician practice. The receiving physician calls the CE and says he destroyed the fax. The CE may be able to demonstrate in its risk assessment that there is a low risk the PHI has been compromised.

Don’t forget that the “safe harbor” still exists. You don’t have a breach if you’ve encrypted data or properly disposed of it according to HHS’ guidance, says Elizabeth H. Johnson, Esq., a partner at Poyner Spruill, LLP.

No definition of ‘compromised’

The final rule has left organizations with some questions. “There is a lot of confusion out there as to exactly what it means for PHI to be compromised,” says Greene. HHS says it plans to issue further guidance to help clarify that question.

One group that had argued for a “compromise” standard rather than a harm standard suggested organizations assess whether data involved in a breach was at “significant risk of being inappropriately viewed, re-identified, re-disclosed, or otherwise misused.” Greene says until HHS offers further clarification, that definition may be as good as any for organizations.

You must document your risk assessment, which needs to be thorough, completed in good faith, and have reasonable conclusions, says Rebecca L. Williams, JD, RN, a partner in Davis Wright Tremaine, LLP’s Seattle office. If an organization decides right away to provide notification of a breach, it does not need to go through the risk assessment process, she says.

How much of a change?

How difficult will this change be for organizations? After September 23, organizations will need to conform to the final rule when evaluating incidents and assessing their breach notification and response obligations.

If you have a good breach risk assessment process in place, you should be in good shape, says Phyllis A. Patrick, MBA, FACHE, CHC, president of Phyllis A. Patrick & Associates, LLC, in Purchase, N.Y.

“The presumption is you have a breach unless you can show otherwise,” she says.

It may be a matter of tweaking an organization’s documentation tools and making sure a risk assessment includes the four factors outlined by HHS, she says. On the other hand, if organizations have not done much to put a breach notification process in place, they will have more work to do.

Chris Apgar, CISSP, CEO and president of Apgar & Associates, LLC, in Portland, Ore., agrees. “If you really look at it, a risk analysis is about determining harm,” he says. Organizations must have a risk analysis process and conduct that analysis consistently every time they review a presumed breach, he says.

Whenever there’s an improper use or disclosure of PHI, the breach “light” needs to automatically come on, says Ruelas. Unless you can show a low probability of compromise, you will need to go through breach notification.

On the other hand, if organization leaders are constantly being notified of possible breach incidents, there may be more effort to correct problems.

One exception removed

Many of the provisions of the breach notification requirements remain the same as they were in the interim final rule.

Incidents that violate the Privacy Rule, that do not meet one of the provided exceptions, and that are not subject to a safe harbor, such as the encryption of PHI, are presumed to be breaches.

The final rule, however, does remove the exception for limited data sets that do not contain birth dates or ZIP codes. The rule now requires that the impermissible acquisition, access, use, or disclosure of limited data sets, even if they do not contain birth dates or ZIP codes, be subject to a risk assessment to demonstrate that breach notification is not required.

Also, if a notice of a privacy breach suggests willful neglect by the CE or BA, then HHS is required to investigate. HHS has clarified that organizations must notify the agency of breaches affecting fewer than 500 individuals within 60 days of the end of the calendar year in which the breach was discovered, not when it occurred, says Williams.
HIPAA Q&A

Public storage units, posting patient info, PHI disclosures

by Mary D. Brandt, MBA, RHIA, CHE, CHPS

Can paper patient records be kept in a public storage unit? The storage company we are considering has a digital entry at the main gate. We would also have a key lock on the storage unit door.

Patient records may be stored in a public storage unit as long as they are secure from unauthorized access. The lock on the storage door unit should be heavy enough to make it difficult to cut off, and you will need to limit keys to a few authorized individuals. Don’t put any identifying information on the door, such as the name of your healthcare facility, so others wouldn’t expect to find patient information there.

It is my understanding that we can make PHI disclosures using our electronic health record (EHR) for payment/treatment/healthcare operations without a consent and that we do not need to track these requests for an accounting of disclosures. Has this changed?

Yes. The ARRA contains additional requirements relating to privacy and security. Title XIII, the HITECH Act, addresses ongoing privacy issues. (See Subtitle D, Part 1, Section 13405 of Public Law 111-5.) Organizations that use an EHR must provide an accounting of disclosures for treatment, payment, and healthcare operations. If you had an electronic record system in place as of January 1, 2009, you have until January 1, 2014, to comply with this requirement. If you acquired an EHR system after January 1, 2009, you must comply by January 1, 2011, or the date on which you acquired the EHR.

One family frequently has a 16- or 17-year-old female bring her 12- and 14-year-old siblings to clinic appointments. Should we treat these children or do we need to have written consent each time from a parent?

It depends on your “consent to treat” process. If you typically have patients (or parents) sign a “consent to treat” form for each visit, you will need to get a parent’s signature on the form before treating. That may be done by faxing the form to a parent and having the parent fax back the signed form. If you don’t get a new “consent to treat” form signed for each visit, you should still contact a parent by telephone to discuss the child’s diagnosis and treatment recommendations each visit. That discussion should be documented in the patient’s record.

Is the UB-04 billing form part of the designated record set according to HIPAA?

Yes. Although HIPAA allows covered entities to define what is included in their designated record sets, the designated record set, by definition, includes medical records and billing records for providers. For health plans, the designated record set includes enrollment, payment, claims adjudication, and case management records.

We are adding an orthopedic clinic to our system. It has a room where up to five patients at a time may be seen for postoperative checks. The physicians and staff discuss treatment plans with the patients, and other patients can hear those discussions. Is this okay?

These are considered incidental disclosures. They are not considered privacy violations, as long as reasonable efforts are taken to limit the information disclosed. Treatment providers should be trained to keep their voices low and avoid discussing sensitive information within earshot of other patients. General conversations are acceptable, such as “It looks like your leg is healing well. Keep the cast on for another two weeks, then return for a re-check. You can bear weight as tolerated.” If patients have questions about their condition or want to discuss sensitive topics, that should be done in a private exam room or office.

I am the privacy officer for a critical access hospital and have a question about psychotherapy notes. Our mental health notes consist of counseling notes for...
overdoses or suicidal patients seen in our hospital or emergency room. A local counselor sees the patient and summarizes his or her findings in a handwritten consult placed in our medical record. Can we release this information as part of our medical record? Are notes from mental health counselors afforded any special protections?

A

HIPAA defines psychotherapy notes very narrowly. They are notes (in any medium) by a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session that are filed separately from the rest of the individual’s medical record. The notes you have described do not meet the definition of psychotherapy notes, so they may be released as part of the patient’s medical record.

State regulations may provide additional protections for mental health records, so be sure to check any additional requirements for your state.

Q

We are considering working with a new bank. A bank representative says there is a new HIPAA rule effective October 1, 2012, that states PHI may not be transmitted via the U.S. Postal Service. He says all insurance payments (because they contain PHI) and explanations of benefits must be sent electronically or via FedEx or UPS if sent on paper. Most of our payments and explanations of benefits are sent EFT/ERA. Do you have any information on this new rule?

A

This is a misinterpretation or over-interpretation of HIPAA or ARRA. Ask the bank representative to show you the specific legal citation that prohibits PHI from being sent by mail.

Q

What is the minimum necessary information that needs to be provided to people regarding HIPAA for public health screening environments?

A

It depends on how the screening is done. Are you collecting and maintaining any information that identifies specific individuals? If you only do noninvasive screening (such as taking blood pressures) and give individuals their results without collecting any identifying information, there is no need to provide a Notice of Privacy Practices. If you are collecting individually identifiable information, it would be reasonable to give individuals a brief notice, perhaps as part of a registration or consent form, that tells them what you will do with the information you collect.

Q

We have two forms for patients who want their information released. One is an authorization form to release information to another person or entity, such as a family member or attorney. The other is an access form that patients complete if they want to review their records or obtain copies. Do we need two separate forms?

A

Using two different forms is acceptable but not necessary. Many healthcare organizations just use an authorization form. If patients want to access their records, they simply complete the authorization form, authorizing release of the information to themselves.

Q

How is the Patient’s Bill of Rights related to the Notice of Privacy Practices (NPP)? Does the Patient’s Bill of Rights relate to hospitals only? Can the two be combined? Should we, as a private practice, provide the bill of rights to a patient in addition to the NPP?

A

The Patient’s Bill of Rights was adopted by the American Hospital Association (AHA) in 1973. It was revised in 1992 and replaced in 2003 with a new AHA document, The Patient Care Partnership, that tells patients what to expect during a hospital stay. For more information, go to www.aha.org.

There is no federal requirement that clinics provide patients with a bill of rights, but several large group practices have posted their patient rights documents on the Internet. To find them, enter “clinic patient bill of rights” into your search engine.

Some states require specific bills of rights for vulnerable patient populations, such as those in nursing homes or those receiving mental health services. To find state-specific laws and regulations, type “(state name) patient bills of rights” into your search engine.

The NPP is a separate document that is required of all covered entities under HIPAA. The NPP tells patients about the information the covered entity collects about them, how that information is used, and their rights with respect to their health information. Since the NPP is usually a fairly long document to meet HIPAA requirements, it may be easier for patients to read a separate document outlining their rights regarding medical treatment.
Security Q&A

Controlling the use of USB drives in hospitals, authenticating patient signatures

by Chris Apgar, CISSP

How can you track or prevent the use of USB drives in a hospital setting?

There are a number of solutions out there that range from generating a simple log of which USB devices were used with your computer to enterprise-level endpoint security solutions. There is a freeware application that will simply track which devices are used with your computer called USBLogView. It is more of a quick-and-dirty solution that will not work well in medium to large organizations because it becomes too labor intense to run reports and review them. It also doesn’t prevent the use of USB drives to store patient information.

The best solution is one that will do three things: control which USB drives can work with hospital computers, limit or eliminate the ability to store data to USB drives, and encrypt the USB drive. Where feasible, look for a solution that will do all three and read a few reviews about the applications you are considering deploying.

A facility received a medical records release form that appears to have been signed by a patient and the patient signature has not been authenticated. The patient contacts the facility by phone and requests that the facility not release her medical records. What is the facility legally obligated to do?

It’s always a good idea to verify the patient before releasing any patient information following receipt of a written authorization. If it’s been determined that the authorization is valid, the patient can at any time revoke that authorization, but revocation must be in writing to be considered valid pursuant to the HIPAA Privacy Rule (164.508[b][5]).

If I were the healthcare provider, I would inform the patient that the revocation needs to be in writing and give the patient an opportunity to submit the revocation within a reasonable length of time.

An affiliated practice has the bad habit of calling three patients back at the same time and requiring the patients to stand in a queue while they are weighed and the weight recorded. The offending physician and the medical assistants have been directed to discontinue this practice. The physician is questioning why. Do you know of a good source?

This represents a violation of the HIPAA Privacy Rule (45 CFR 164.530[c][2]). The physician is responsible for limiting incidental disclosure of PHI—in this case, limiting disclosure of one patient’s weight to another patient. Also, this borders on a breach of unsecured PHI. The same section of the Privacy Rule that addresses limiting incidental disclosures also requires covered entities to protect against violations of the Privacy Rule—in this case, unauthorized disclosure of a patient’s weight to another patient.

This also represents a violation of what has been called the “mini-security rule” (45 CFR 164.530[c][1]). The rule requires adoption of administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of PHI in any form. In this case, the physician is violating the administrative safeguard of access control.

The physician is required to reasonably ensure access to PHI is limited to those with a “need to know.” Other patients don’t have a need to know when it comes to another patient’s weight.

This could also be interpreted as a violation of the HIPAA minimum necessary requirement (45 CFR 164.502[b]).

It’s true that disclosures for treatment represent an exception from the minimum necessary requirement, but that applies to disclosures made between covered entities for the purpose of treatment. In this case, the disclosure is to other patients and does not represent sharing PHI for treatment purposes. When all is said and done, this physician is violating several provisions of the HIPAA Privacy Rule.
Tips from this month’s issue

HHS releases HIPAA Omnibus Rule (p. 1)
1. The final rule implements most of the privacy and security provisions of HITECH and extends the reach of HIPAA.
2. With a few exceptions, organizations must comply with the final rule by September 23—180 days after publication.
3. The final rule addresses a number of privacy issues related to the uses and disclosures of PHI, such as communications for marketing or fundraising, exchanging PHI for remuneration, disclosures of PHI to persons involved in a patient’s care or payment for care, and disclosures of student immunization records.
4. The rule includes the expansion of the use and disclosure of PHI for fundraising purposes.
5. The final rule expands an individual’s rights to access electronically stored PHI.
6. The final rule also allows patients to restrict information for out-of-pocket payments.
7. The final rule changes the requirements for what organizations must include in their Notice of Privacy Practices.
8. Business associates (BA) and their subcontractors are now subject to civil money penalties and other enforcement actions for noncompliance with applicable provisions of HIPAA.

Ten steps to help you comply with the HIPAA final rule (p. 5)
9. By conducting a risk analysis, you will determine what specific risks your organization faces.
10. Review your existing Notice of Privacy Practices and be sure you address the additional patients’ rights included in the final rule.
11. Read the rule and perform a gap analysis to determine what policies and procedures you need to revisit in light of the changes.
12. Develop a strategy for providing copies of electronic records to patients.

HIPAA becomes reality for BAs, subcontractors (p. 7)
13. With the final rule, responsibility to protect PHI now rests on BAs and their subcontractors.
14. BAs now have direct liability under the Omnibus Rule for impermissible use and disclosures of PHI and must notify covered entities (CE) of a breach.
15. HHS has modified the rules to provide that BAs may “create, receive, maintain, or transmit” PHI on behalf of a CE.
16. Under the final rule, subcontractors of BAs are, by definition, now themselves considered BAs if they create, receive, maintain, or transmit PHI.

‘Harm threshold’ eliminated (p. 8)
17. Under the final rule, HHS eliminated the controversial “harm threshold” that required the reporting of a breach if there was a significant risk of financial, reputational, or other harm to affected individuals.
18. Breach notification is necessary unless a CE or
BA can demonstrate, through a documented risk assessment, that there is a low probability that the PHI has been compromised.

The rule now requires that the impermissible acquisition, access, use, or disclosure of limited data sets, even if they do not contain birth dates or ZIP codes, be subject to a risk assessment to demonstrate that breach notification is not required.