Long-term care facilities face additional challenges to protect resident privacy

If many acute care hospitals struggle to protect patient privacy, long-term care organizations face their own challenges in ensuring the privacy of residents who live in their nursing homes and assisted living facilities.

“We are subject to a complexity that makes privacy more difficult,” said Drew Graham, Esq., an attorney in Hall Booth Smith, PC’s aging services group in Atlanta. Many residents call these facilities home and receive regular visits from family members. Staff members also get to know these individuals well, frequently interacting with them daily to provide care.

Yet most long-term care facilities are not exempt from the same HIPAA rules as other healthcare organizations. The so-called HIPAA mega rule, released January 17 by HHS, also applies to long-term care organizations, said Brittany H. Cone, Esq., CHC, an attorney at Hall Booth Smith.

Graham and Cone spoke during HCPro’s webcast, “HIPAA Privacy Across the Continuum of Long-Term Care: Maintaining Privacy in a Non-Private Environment.”

Let’s look at some of the challenges long-term care organizations face.
Quick Hits

Online

OCR publishes new tools to educate consumers about HIPAA

OCR has developed new materials to educate consumers and healthcare providers on HIPAA privacy and security. OCR has posted a series of fact sheets, also available in eight languages, to inform consumers about their rights under the HIPAA Privacy Rule. These materials are available on OCR’s website. The fact sheets compliment a set of seven consumer-facing videos released earlier this year on OCR’s YouTube channel.

http://blogs.hcpro.com/hipaa

OCR: More guidance coming on HIPAA mega rule

OCR will be providing additional guidance on the HIPAA mega rule, the all-in-one HIPAA game-changer published in the Federal Register in January. Health IT Security reported April 26 that HHS attorney Iliana Peters said the department will be offering the additional guidance.

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.

From the Field

“We are subject to a complexity that makes privacy more difficult.”

Drew Graham, Esq.

“The required modifications dictated by the final rule are very likely to require redrafting Notices of Privacy Practices.”

Elizabeth H. Johnson, Esq.

Follow Us

Follow and chat with us about all things healthcare compliance, management, and reimbursement.

@HCProInc

Questions? Comments? Ideas?

Contact Senior Managing Editor Jay Kumar at jkumar@hcpro.com or 781-639-1872, Ext. 3144.
Compliance with new HIPAA rules

The HIPAA omnibus final rule is enforceable for all covered entities (CE) beginning September 23, 2013. Like acute care hospitals, long-term care facilities must come into compliance with the new rules quickly, said Cone.

They face the same major changes brought about by the mega rule:
- Elimination of the “harm threshold” for determining whether a breach occurred
- Expansion of the definition of business associate
- Expansion of individual rights and authority to medical records
- The need to modify a CE’s Notice of Privacy Practices (see related story on p. 7)

All of these changes will require CEs to update their policies and procedures to ensure compliance with the new rules.

“Our suggestion to providers is to go ahead and start taking actions today,” said Cone. Organizations face fines of up to $50,000 per violation for failure to comply with the HIPAA rule. (See the story on p. 5 for a more detailed look at the changes LTC organizations must make.)

“The enforcement aspects of HIPAA and the regulatory exposure created by it are huge,” said Graham.

Issues for LTC providers

“A lot of providers feel overwhelmed,” Graham said, in reference to the HIPAA requirements. Nursing homes need to be concerned about protecting resident privacy when care is provided to residents by other providers, including hospitals, physicians, and therapists, he said.

- Surrogate decision-makers. One issue that long-term care organizations face is when decisions have to be made by surrogate decision-makers on behalf of a resident.
  - HIPAA allows a CE to use or disclose PHI as follows:
    - To the individual
    - For treatment, payment, or healthcare operations
    - Pursuant to an authorization
  - The organization needs to know who has authorization to use or disclose a resident’s information. Who can consent to a resident’s treatment on admission, during residency, and if there are record requests or any litigation?
  - Issues often arise in the context of an involuntary discharge or a resident’s refusal of care, Graham said. Keep in mind the main focus of HIPAA is the protection of the individual, he added.
  - “Don’t be fearful of a breach of HIPAA to the point you compromise resident care in any way,” he advised.
  - When it comes to surrogate decision-makers, be sure you know your state law and comply with it, Graham said.
  - Nursing homes frequently have questions about how to deal with a family member who has been a resident’s leading caregiver but who does not have power of attorney or is not authorized to make decisions. “It’s a state-by-state issue,” he said.
  - Ask for documentation if someone says they have the authority to make decisions on behalf of a resident; a verbal statement is not enough, Graham said.

- Granny cams. Another privacy issue that long-term care organizations must confront involves the use of “granny cams.” These are cameras that family members set up in a resident’s room to record all activity, including possible signs of elder abuse.
  - Some states—including Texas, New Mexico, and Maryland—have laws in place to allow such cameras, Graham said.
  - Use of these cameras raises concerns about the rights of staff members and facilities, who argue that their own rights are being violated.
  - “I’ve seen this issue come up a lot lately,” said Graham.

- Privacy rights get stickier in the case of shared rooms, Graham said.
  - If a granny cam is used, you may want to make it a policy to post and maintain a notice that electronic
monitoring is taking place, he said.

“We suggest the issue be well documented within the resident record,” Graham said.

- **Social media.** Just as in other healthcare organizations, social media has created privacy challenges for long-term care facilities as well, Graham said.

  Social media has been the culprit behind plenty of PHI breaches recently.

  Long-term care facilities need to balance the protection of residents’ privacy while allowing staff certain freedom.

  “My sense is that providers are under the impression that they owe their employees more freedom than they actually do,” Graham said. Facilities should look closely at what freedoms they provide when it comes to social media.

  Address the use of social media in your policies and procedures. “At a bare minimum, you need a policy on the use of company equipment to access the Internet,” Graham said.

  Make it clear to employees that there is no expectation of privacy on company-owned computers or if they connect to a facility’s Wi-Fi, he said.

  One research group estimates that 40% of American adults access websites via their cell phones. That means employees can access sites without any control by facilities.

  You can say without reservation that if employees use their own device to log on or connect to a facility’s Wi-Fi, there is no expectation that communications or personal email accounts will be private, Graham said.

  There is also a risk that staff will post PHI on social media sites such as Facebook, Instagram, LinkedIn, or Twitter, as well as blogs and discussions forums. A hospital in Michigan hired a worker who posted information about an emergency room patient.

  Ensure that your employees understand the penalties associated with HIPAA violations and that residents are entitled to protection of their privacy.

  Absolutely prohibit the disclosure of PHI on social sites, Graham said. Make it clear that employees may not use company logos or trademarks.

  Be sure employees understand that even if they do not identify residents by name, a posting could contain PHI. Disclosure of certain information could reveal a patient’s identity even if no name is given.

Prohibit anyone from linking from a personal Web page back to the long-term care community in any way, Graham said.

  Facilities can block access to social media sites just as some schools do, Graham added. “Take a hard look at what you want folks to access, including your residents.” You can make it clear that use of social media during working hours is absolutely prohibited, he said.

  Tell employees to be cautious about “friending” residents or family members.

  But even if you block access to sites at your facility, there is still a risk from employees using their own private accounts.

  Facilities can adopt a policy requiring employees to indicate they are speaking for themselves, not for the company, if they post information about their jobs, he said.

  Be cautious about your facility’s use of social media for marketing purposes. Facilities want to create a home-like environment and a happy workplace, and during festive times, staff members may have the impulse to take photos of happy residents, Graham said. “We recommend you absolutely prohibit the taking of photos or video at company events or inside your facility without express authority,” he said. Consider having a designated person who is well versed in HIPAA take any photos or video.

  “You can’t have staff taking pictures even if they are well intentioned,” he said. You can easily lose control of what happens to these photos. They may be posted on the Internet or used without permission.

  Take time to explain to staff why you are prohibiting photos. “Some of these [restrictions] may be difficult to stomach, but you need to think seriously about it,” he said.

- **Be smart about smartphones.** Be sure employees use password protection on their smartphones if they are sending or receiving electronic health records.

  Without password protection, a lost cell phone containing medical records could spell trouble, allowing anyone to access that PHI.

  So put a policy in place requiring employees to have a password on their smartphones if they are sending or receiving electronic records.
A closer look at the mega rule

The so-called HIPAA mega rule has required numerous changes by healthcare organizations.

Let’s review the major changes that organizations, including long-term care facilities, must address.

- Breach notification changes. The mega rule did away with the harm threshold that existed under HHS’ interim final rule on breach notification. Under the interim rule, covered entities (CE) and business associates (BA) could avoid notifying patients or residents of a breach when the entity determined a use or disclosure of PHI did not pose significant harm to the individual, said Brittany H. Cone, Esq., CHC, an attorney in the aging services group at Hall Booth Smith, PC, in Atlanta. Cone spoke during HCPro’s webcast, “HIPAA Privacy Across the Continuum of Long-Term Care: Maintaining Privacy in a Non-Private Environment.”

Now under the final rule, entities must conduct a risk assessment when determining whether a breach occurred, considering at least the following four factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification. “In other words, what is in that data?” said Cone. Does it include names and Social Security numbers? Is it sensitive health information, such as mental health records. Is it financial data that could lead to identity theft?
- The unauthorized person who used the PHI or to whom the disclosure was made. Was the data acquired by a criminal who is likely to use it for fraud? Or was it sent to the pharmacy by accident?
- Whether the PHI was actually acquired or viewed. If PHI was sent by email to the wrong recipient, was it opened and read? If a laptop computer was stolen, do forensics indicate the data was not viewed?
- The extent to which the risk to the PHI has been mitigated. Were you able to obtain confirmation from the person who received a missent email that he or she deleted it and will not use the information in any way?

While HHS is not calling it harm, organizations still must consider the harm to residents in a risk assessment, Cone said. The focus is on the PHI itself and there is now a presumption of breach unless your analysis proves otherwise, she said.

- A new definition of BA. Before the mega rule, if a healthcare provider contracted with a BA who handled its PHI, and that BA in turn hired a subcontractor who also used or disclosed PHI, the subcontractor was not directly responsible for complying with HIPAA, Cone said.

Now, however, third-party subcontractors, not just direct BAs of healthcare providers who use and disclose PHI, are held accountable, she noted.

BA contracts must be updated within 180 days of January 25. So organizations should begin to review and update those agreements as soon as possible. (See p. 6 for a list of some of the elements that long-term care organizations should include in those contracts.)

Be sure your BAs have protections in place so your PHI is protected. Also, ensure BAs have corresponding agreements with their subcontractors who also are responsible for protecting PHI, Cone said.

You may have contracts that have been in place for years, said Drew Graham, Esq., also an attorney at Hall Booth Smith. However, be sure the new elements and language are added into your contracts as you go forward.

- More individual rights and authority regarding medical records. The mega rule makes several changes on this front. It allows patients and residents to ask for a copy of their electronic medical record in an electronic form, Cone said. It gives residents who pay by cash the authority to instruct their provider not to share information about their treatment with their health plan. It also sets new limits on how information is used and disclosed for marketing and fundraising purposes. And it prohibits the sale of an individual’s health information without his or her permission.

- Modifications needed to the Notice of Privacy Practices. The notice must now include the following:
  - A description of activities involving uses or disclosures of PHI that require an individual’s authorization.
  - Notice that individuals have a right to opt out of receiving fundraising communications.
  - A statement explaining that CEs are required by law to notify affected individuals following a breach of unsecured PHI. This places a greater obligation on providers, said Cone.
HIPAA checkup
How compliant are you?

Are you HIPAA compliant? Here are some questions long-term care organizations can ask themselves, according to Drew Graham, Esq., and Brittany H. Cone, Esq., CHC, attorneys in the aging services group at Hall Booth Smith, PC, in Atlanta:

• Have you designated a HIPAA officer? This is extremely important, said Cone. This person provides oversight of your facility’s HIPAA program. Any time there is a HIPAA-related question, this is the person you can go to. Your HIPAA officer will oversee the updating of policies and procedures and is the go-to person to conduct a risk assessment of a potential breach.

• Have you addressed business associate (BA) agreements? Are you sharing medical records with other associates? If it is for treatment and payment purposes—for instance, with hospitals, therapists, or pharmacists—you may not need a BA agreement, said Cone. On the other hand, if you have an IT company that has access to PHI, you will need a BA agreement.

• Do you have access and termination procedures? Remember that you need to protect both ePHI and your paper records, said Cone. If employees don’t need access to PHI to do their jobs, you should restrict that access, she said. For example, a janitor should have access to a computer that contains PHI only if he needs that access to do his job. Be sure your computers are password protected and those passwords are strong. For example, require passwords to have a minimum number of characters, capital letters, and symbols so that they cannot be easily guessed. Be sure when your organization terminates any employee, his or her access to PHI is terminated immediately.

• Do you conduct risk assessments and audits? Do a risk assessment at least twice a year to identify risks to PHI, said Cone and Graham. If you identify an issue, be sure you take corrective action.

• Do you comply with the “minimum necessary” standard? This means you disclose the minimum necessary information. For instance, if an insurance company has a question about a resident’s care, your organization may not need to disclose the entire medical record. Provide only the information needed to address the question being asked.

• Do you have locked storage for your records? Where are your records kept? Are they behind a desk where someone can easily gain access? You could have a potential HIPAA violation. Be sure records are stored in a locked area.

• Do you use access codes? You want to ensure that only those who need access to your records can log on to computers.

• Do you have policies and procedures related to employee hiring and termination? It is vital to make sure when an employee is no longer working at your facility that his or her access to PHI is terminated. You do not want a former employee to be able to take records out of the building or access your computer records. When employees are terminated, have a process in place so they no longer have access to your records, such as disabling a password.

Suggested elements to include in your BA agreements

Like other healthcare organizations, long-term care organizations will need to review and update their business associate (BA) agreements to comply with the HIPAA omnibus final rule.

Below are some of the elements that Brittany H. Cone, Esq., CHC, and Drew Graham, Esq., attorneys with the aging services group at Hall Booth Smith, PC, in Atlanta, suggested organizations include in their agreements with BAs pursuant to the final rule:

• Establish the permitted and required uses and disclosures of PHI by the BA
• Provide that the BA will not use or further disclose the
Make modifications to Notice of Privacy Practices to comply with final HIPAA rule

One task that almost every healthcare organization is going to have to tackle to comply with the HIPAA omnibus final rule is amending its Notice of Privacy Practices (NPP).

The final rule—released by HHS on January 17 and dubbed the “mega rule”—changes the requirements for what organizations must include in their NPP.

“The required modifications dictated by the final rule are very likely to require redrafting Notices of Privacy Practices,” says Elizabeth H. Johnson, Esq., a partner at Poyner Spruill, LLP.

HHS states that covered entities (CE) do not have to update notices if they already made changes to implement HITECH, provided the provisions in their current notices are consistent with the final rule’s requirements, Johnson says. However, organizations are unlikely to have anticipated several of the modifications described in the final rule and these may not have been taken into account in updated versions of notices, she cautions.

Therefore, undertake a thorough review to be sure your notice is in compliance.


Get going now

CEs have until September 23 to comply with the final rule requirements for NPPs.

“In my view, there is no better time to look at the Notice of Privacy Practices and ensure it is compliant, not only with previously required elements, but elements incorporated as part of the final rule changes now,” says Frank Ruelas, MBA, principal of HIPAA College in Casa Grande, Ariz. “What better motivation is there to make sure your NPP is in alignment with the rules?”

In some cases, healthcare organizations may not have looked at their NPP in years. In many cases, the current privacy officer may not have been involved in drafting the original NPP, Ruelas says.

Your revisions will need to address breach notices, restrictions on use and disclosure of PHI, access to PHI, and other updates, he says.

Organizations should make sure their NPP accurately describes their actual privacy practices, says Rebecca L. Williams, JD, RN, a partner in Davis Wright Tremaine, LLP’s Seattle office. In other words, be sure it reflects the omnibus rule changes, but also your
day-to-day operations.

Go through and make sure you have addressed specific requirements and be sure you update forms and other documents, she says.

**The key provisions**

Several of the rule changes implemented by HHS necessitate corresponding changes to the NPP, says Johnson. Here are a number of key provisions that CEs must address based on the final rule:

- Include a description of uses and disclosures that require an individual’s authorization, says Johnson. This will include use or disclosure for marketing, selling PHI, and use or disclosure of psychotherapy notes (if applicable). The NPP should include a statement that other uses and disclosures not described in the notice will be made only with the individual’s authorization. As previously required, include a statement that the individual has the right to revoke an authorization.
- The notice must describe uses and disclosures of PHI for fundraising, and note the individual’s right to opt out of such uses and disclosures, Johnson says.
- For CEs that are health plans and intend to use PHI for underwriting purposes, the NPP must advise individuals that the CE is prohibited from using genetic information for underwriting purposes, she says.
- The NPP must advise individuals of the CE’s legal obligation to notify them if their PHI is affected by a security breach, she says.
- Notices made available by healthcare providers must describe the individual’s right to request restrictions of disclosures to health plans for payment or healthcare operations regarding services for which they have paid in full out of pocket.
- HHS has modified the method by which health plans (but not healthcare providers) must notify participants of material changes to their NPP, says Johnson. Health plans that post their notices on their websites may prominently post the change or its revised notice. Then in its next annual mailing, the health plan must provide the revised notice, or information about the material change and how to obtain the revised notice. Health plans that do not post their notice on their websites must provide the revised notice, or information about the material change and how to obtain the revised NPP, to participants within 60 days of the revision. Health plans are still required to remind participants of the availability of the notice at least once every three years. There is no change for providers on distribution requirements.

**What the provisions mean to CEs**

Assuming the newly required disclosures are not included in your current notice, you must implement the updates mandated by the final rule, Johnson says.

The modifications will constitute material changes, meaning that CEs must promptly post or redistribute their notices before or on the compliance date.

Providers should post the revised NPP and health plans will be required to republish or recirculate their notices in one of the ways permitted by the final rule, as described above.

Although the notice must alert individuals of their right to opt out of fundraising communications, the NPP does not need to describe the mechanism by which individuals can exercise that right. Rather, you should include or describe the opt-out mechanism in the fundraising communication, Johnson says.

HHS indicates that CEs may use “layered notices,” such as a short-form notice supported by a full notice, if the notice delivery requirements of the final rule are otherwise fulfilled, she says.

HHS has retained the requirement for individuals to opt in before they may receive notices electronically, such as via email, in lieu of the usual distribution requirements, she says.

One element that HHS no longer requires in the NPP is a statement if the CE intends to contact the individual to provide appointment reminders or information about treatment alternatives, says Williams.

**A cause for confusion**

The requirements about the redistribution of NPPs has created a lot of confusion, says Ruelas. “If you read the final rule, it clearly states that CEs that are not health plans do not need to redistribute the Notice of Privacy Practices.”

While some attorneys are advising clients to
briefings on HIPAA

require the individual to have to ask the receptionist for a copy of the full NPP.

Although organizations may provide a summary to make it easier for patients, they may unknowingly place a burden on themselves. “Be very careful how you proceed,” Ruelas says.

While it ordinarily would be true that providers do not need to recirculate their revised NPP to existing patients, Johnson cautions it may not be true in every case. An exception is where a CE chose to state in its notice that it would redistribute the NPP in the event of material changes.

“In other words, if the CE promised redistribution in a past notice, then the CE needs to keep that promise,” she says. While it is not required by HIPAA, it would purely be a function of the enforceability of the promises made to consumers in previous notices.

So know what your NPP says about distribution of revised notices and be sure you comply with your own document.

redistribute revised NPPs, if you are not a health plan, that is not a requirement, Ruelas says.

“You simply need to post it in a clear and prominent place for existing patients and make it available upon request,” he says. For instance, a patient can ask the receptionist for a copy. Provide new patients with the revised NPP.

Some healthcare organizations, as a convenience to patients, like to have a “layered” notice, Ruelas says. It provides a short summary of the changes made to the NPP, which allows patients to see what changes occurred without looking through the entire notice.

“You can do that, but here’s the curveball,” he says. If you use a layered approach and post a summary of the notice, the final rule states clearly that you must make the full notice immediately available. For instance, you must provide copies of the NPP on a table directly under the posted summary for individuals to pick up without any additional burden on their part, the final rule states. It would not be appropriate to

Remind your workforce members to ‘zip their lips’ when it comes to patient privacy

In a time when so much attention is focused on issues such as cyber security and the dangers posed from evolving technology, it’s easy to forget the HIPAA basics, such as the need for workforce members not to gossip or chitchat about patients with other staff members or people in the community.

One reminder of that came on a HIPAA listserv recently with a lively exchange of comments about whether a hospital staff member created a HIPAA breach by talking about a patient with a neighbor. Opinions differed about whether the exact circumstances constituted a breach, but the lesson for Greg Young, information security officer at Mammoth Hospital in Mammoth Lakes, Calif., was clear: Healthcare organizations need to keep up their efforts to provide staff with ongoing privacy education to prevent the kind of gossip that created the potential violation.

Proof is in the pudding

Young and other HIPAA leaders agree that one of the subjects that seldom gets enough attention during workforce training is personal and professional boundaries.

Young says he’s written more than 75 articles for Mammoth’s employee newsletter over the past six years and it has become a staple of ongoing privacy education. And he has solid evidence that all of that education has paid off.

Back in January, Young took a hard spill on the ski slope and landed in the emergency department (ED) at his own hospital with a back injury. For several weeks after his trip to the ED, he was telling people what happened to him and they had no clue about his injury, which left him temporarily paralyzed. People in the ED, in the imaging department, in billing, and the rest of the departments he had contact with did not chitchat about his being brought into the hospital with a possible broken back.

“So I feel all the education over the years has helped to create a climate of security, or as I refer to it, a web
of security,” he says.

A fight against complacency

Dena Boggan, CPC, CMC, CHPC, HIPAA privacy and security officer at St. Dominic Jackson (Miss.) Memorial Hospital, says healthcare organizations need to constantly reinforce HIPAA basics with their workforce.

“This is the top nemesis for privacy officers everywhere—complacency,” she says. “I am a firm believer in always going back to the basics when providing initial training in orientation, as well as continued reinforcement throughout the year—every year.”

The requirements for training have not changed, even though the technology has, Boggan says. It’s not so surprising why there is not as much emphasis on the simple basics of compliance as there once was. HIPAA privacy and security officers have been focused on the threats from evolving technology, new regulations brought about by the HITECH Act, the need to address meaningful use, and more, she says.

“We’ve been inundated with new and evolving regulations so much in the past four years alone, we can barely breathe, much less concentrate on covering every nuance of training that’s necessary and required,” Boggan says.

However, not reinforcing lessons for your staff can be dangerous, she says. Complacency among staff occurs at all levels of employment and with both long- and short-term employees, she says. When incidents arise, Boggan says she learns on investigation that employees have indeed received HIPAA training.

It leaves her shaking her head and asking, “What happened here?” “Not once have I had an employee state, ‘I never received training’ or ‘I didn’t know’—it’s always ‘I forgot,’ ” she says. “It’s frustrating because we incorporate a number of processes here to make sure this all stays fresh in our employees’ minds, including weekly emails to all staff with scenarios and reminders.”

Make training specific

HIPAA training must keep reinforcing basics, agrees Nancy Davis, MS, RHIA, director of privacy and security officer at Ministry Health Care in Wisconsin.

Like Young, she touches on the topic in employee newsletter articles. A recent article titled “Don’t Ask, Don’t Tell” was a reminder to staff not to ask questions about patients that they don’t need to know to carry out their job duties (e.g., Who did the ambulance just bring in? Did the patient in 222 have her baby yet?) and not to divulge information if asked.

Ministry Health Care also recently retooled all staff privacy and security computer-based training and focused on scenarios. To develop those realistic scenarios, Davis went back and audited the past three years of privacy investigations and targeted problematic situations. She also solicited concerns from local privacy and security officers so that computer-based training is less focused on the academics of privacy and more on the practical applications. So far, feedback from staff has been good, she says.

It’s also important to remind staff what to do if they see a privacy violation, says Boggan. “Just two days ago, I had an employee call me, concerned about a conversation she overheard. A nurse stated though she’s never personally witnessed a privacy violation, she wouldn’t know who to call if she did. I thought, ‘Are you kidding me here?’ ”

Fighting human nature

Boggan says incidents where staff violate patient privacy by talking about patients doesn’t happen often. “But yes, complacency rears its ugly head from time to time, and it will always be a perennial problem to deal with. It is human nature,” she says.

Young agrees it is an issue privacy and security officers will always have to educate workforce members about. Most of the time, individuals are not trying to be deceptive or mean. “They were just being human,” he says.

Young says he has had to address situations over the years including one in which a nurse went to the laboratory to have a pregnancy test, which turned out positive. In a short time, three other employees either congratulated her or, in one case, gave her a list of health dos and don’ts. The nurse was not pleased with the attention and rightfully so.

In another case, an employee entered a patient’s room and observed the patient was a child of another employee. A little later, a third employee approached the child’s parent to wish her well. However, the parent
was not happy that an employee, who had no reason to know her child was in the hospital, had found out.

Facilities must address the problem by creating a positive atmosphere across the organization and making inappropriate discussion of patients unacceptable behavior, Young says.

**Follow sanction policies**

In addition to educating staff, organizations need to follow their sanction policy, Boggan says.

“You hold the individual accountable. Word of mouth among employees about another employee receiving a sanction for ‘I forgot’ does wonders,” she says.

First of all, the sanctioned employee is going to remember the repercussion from his or her action, and colleagues of that employee will sit up and pay attention quickly, Boggan says.

“Inappropriate disclosure of PHI, whether it’s oral, written, or electronic, is unacceptable, period. There should not be any lesser repercussion simply because the disclosure was oral—it is still a violation,” she says.

It’s also important to hammer home the severe consequences that can result from staff members’ actions, including enforcement action against an organization for a HIPAA violation, says Brandon Ho, CIPP, HIPAA compliance specialist at Pacific Regional Medical Command and Tripler Army Medical Center, part of the Military Health System, in Honolulu.

“[I tell staff], no matter what context you think you are in, others will always see you as a healthcare professional first,” he says.

“So you may think that you are talking socially, gossiping, just chitchatting … but if you are reported for disclosing information without authorization, you could be jeopardizing your career.”

Someone could easily bring an unauthorized disclosure of their information to the attention of the facility’s privacy officer or they could make a complaint to OCR, which then might be investigated. “Your hospital, clinic, or office could become the subject of an OCR/HHS audit and no one will thank you for that,” Ho says.

In classroom sessions to educate staff about HIPAA and periodically through email blasts, Ho says he impresses on employees the seriousness of violations. Often supervisors will print the email blasts and post them in staff common areas to assist in getting the word out, he says.

---

**A sample article**

One way to educate your staff members about HIPAA privacy and security is through an employee newsletter.

**Greg Young**, information security officer at Mammoth Hospital in Mammoth Lakes, Calif., has been writing articles for his facility’s employee newsletter for years. Here is an excerpt from an article he wrote reminding staff members not to engage in small talk about patients. Young says organizations can adapt the article for use at their own facility.

*In healthcare we have to be especially guarded about our “small talk.” This is even truer between each other. It is easy to imagine why two employees within our walls might feel safe talking about a patient’s information. But the fact is we shouldn’t be having that conversation unless it directly pertains to our job. Let’s say that again. It “directly pertains to our job.” In the course of doing our job we see a lot of sensitive personal information about patients. And the patients very often include our own employees. We may see information that we personally find shocking, surprising, and even questionable when measured against our own personal standards. But none of those reasons are good enough to “chit-chat” or “small talk” with others. We do our jobs and that is it. You don’t turn to your co-worker and small talk about what you have seen, heard, or read. Keep in mind that all this extends beyond work. Even though you are not paid for your time away from work, you are responsible for protecting the knowledge acquired at work that you take with you when you leave. So too, your reputation when you leave work. You are expected to maintain exceptional integrity as a result of the trust placed in you when you accepted a job in healthcare.*
Absio Corporation offers ePHI encryption support

Demonstrating that ePHI encryption meets the safe harbor requirements may be more difficult than it seems when planning for that inevitable breach. Full disk encryption may not be enough. Many healthcare users believe encryption software installed on mobile devices and desktops will avoid the potentially damaging breach notification. The question is: Can you prove ePHI was encrypted at the time the device was lost, accessed, or stolen? Absio Corporation may have the answer.

Absio supports secure messaging, storage, and data sharing in a way that meets the safe harbor standard. Its solution also provides healthcare organizations the ability to prove that ePHI was fully encrypted at the time of a breach. This is true whether ePHI is sent via email or stored on mobile devices.

Absio’s solution appears to be the only platform that is designed to protect ePHI wherever it travels. This includes the ability to control where any ePHI is transmitted to and when it is then forwarded. The solution supports control over the data, allowing the sender the ability to control whether the ePHI can be copied, pasted, printed, and forwarded. This is true for smartphones, tablets, laptops, and personal computers.

The solution can be hosted by Absio or by the end user, such as a hospital, a business associate, or a payer. Use of the platform to support encryption of all ePHI in a data center means the encryption keys can’t be accessed even by data center employees. If used and installed properly, the solution eliminates a major source of data leakage or breaches.

So how does it work? All of the data is wrapped in what is called an object created using Secure Extensible Global Content Object. Each “object” is individually encrypted and contains the content and its metadata or data describing the data, and any rules around how ePHI may be used or transmitted.

Encryption and decryption is done on the mobile device or desktop rather than on those servers in the data center. Absio has been around the military and intelligence community for some time and supports a level of encryption that would be acceptable to entities such as the National Security Agency. The method of encryption has been government approved and is consistent with the National Institute of Standards and Technology standards (FIPS 140-2).

Absio is in the business of selling identities that have been verified. Often you don’t really know who the person on the other end is when logging on to a Facebook page or starting a video chat with Skype. This solution supports the ability to validate or authenticate the person on the other end of the information exchange. This is important when sharing ePHI and to demonstrate compliance with the HIPAA Privacy and Security Rules (45 CFR § 164.312(d) and 45 CFR § 164.530(c)).

Absio supports secure messaging and collaboration between healthcare organizations. It allows ePHI “owners” to ensure the ePHI can only be viewed by authorized individuals as well as only allowing those individuals to use the ePHI as permitted by the “owner.” It also protects against unauthorized access to that healthcare organization’s network versus accessing the network and all of the information stored on that network.

One of the keys to protecting ePHI is making sure it cannot be accessed when it is stored locally or on a mobile device or desktop. Absio’s solution assigns an individual identity that allows your workforce to have a single account that can be used to secure multiple devices such as a desktop and a tablet. It also supports the ability to synchronize data between those devices in a way that is both simple and secure. The solution secures that ePHI whether a workforce member is signed on to the network or Internet or offline. When the workforce member signs on to the network again, the data stored on that mobile device or desktop is synced with the network. Absio offers a secure solution to data storage and transmission and provides the ability to demonstrate healthcare organizations have met the safe harbor standard. This prevents misuse of ePHI and the requirement to notify OCR. Also, this solution allows healthcare organizations to better manage the use of ePHI, whether it’s preventing a recipient from printing that information or sending it on to someone else.
Tips from this month’s issue

**Long-term care facilities face additional challenges to protect resident privacy (p. 1)**

1. The so-called HIPAA mega rule, released January 17 by HHS, also applies to long-term care organizations.
2. The HIPAA omnibus final rule is enforceable for all covered entities (CE) beginning September 23, 2013.
3. Organizations face fines of up to $50,000 per violation for failure to comply with the HIPAA rule.
4. One issue that long-term care organizations face is when decisions have to be made by surrogate decision-makers on behalf of a resident.
5. If a granny cam is used in a patient room, you may want to make it a policy to post and maintain a notice that electronic monitoring is taking place.
6. Address the use of social media in your policies and procedures.
7. Ensure that your employees understand the penalties associated with HIPAA violations and that residents are entitled to protection of their privacy.
8. Be sure employees use password protection on their smartphones if they are sending or receiving electronic health records.

**Make modifications to Notice of Privacy Practices to comply with final HIPAA rule (p. 7)**

9. Designate a HIPAA officer to oversee the updating of policies and procedures and be the go-to person to conduct a risk assessment of a potential breach.
10. Address business associate agreements, especially if you’ve got an IT company that has access to PHI.
11. Have access and termination procedures in place to protect both electronic PHI and your paper records.
12. Do a risk assessment at least twice a year to identify risks to PHI.
13. Ensure that your records are stored in a locked area.
14. Have policies and procedures in place related to employee hiring and termination.
15. HHS states that CEs do not have to update notices if they already made changes to implement HITECH, provided the provisions in their current notices are consistent with the final rule’s requirements.
16. Your revisions will need to address breach notices, restrictions on use and disclosure of PHI, access to PHI, and other updates.
17. Include a description of uses and disclosures that require an individual’s authorization.
18. The notice must describe uses and disclosures of PHI for fundraising, and note the individual’s right to opt out of such uses and disclosures.
19. The NPP must advise individuals of the CE’s legal obligation to notify them if their PHI is affected by a security breach.
20. Notices made available by healthcare providers must describe the individual’s right to request restrictions
of disclosures to health plans for payment or health-care operations regarding services for which they have paid in full out of pocket.

### Remind your workforce members to ‘zip their lips’ when it comes to patient privacy (p. 9)

**21.** Healthcare organizations need to keep up their efforts to provide staff with ongoing privacy education to prevent the kind of gossip that creates potential violations.

**22.** Healthcare organizations need to constantly reinforce HIPAA basics with their workforce.

**23.** Facilities must create a positive atmosphere across the organization and make inappropriate discussion of patients unacceptable behavior.

**24.** Hammer home to staff members the severe consequences that can result from their actions, including enforcement action against an organization for a HIPAA violation.

---

**Privacy and Security Primer** is a monthly, two-page Briefings on HIPAA insert that provides background information that privacy and security officials can use to train their staff. Each month, we discuss the privacy and security regulations and cover one topic. June 2013.