 Contents

3  Baptist Healthcare Bans SSNs to Reduce Risk, Please Patients

4  Congress Orders the Removal of SSNs From Medicare Cards

5  New Ponemon Report: Covered Entities Lack Resources, Staff

8  OCR Offers Guidance on, EEOC Explains HIPAA and Workplace Wellness

9  Harris Poll: Breaches, Not Compliance, Now Drive Health Care IT Spending

11 Privacy Briefs

OCR Audits Take a Small Step Forward; for Covered Entities, No News Isn’t Good News

The wheels of the government are slowly grinding toward the start of the HHS Office for Civil Rights’ (OCR) audit program. OCR has been granted approval by the Office of Management and Budget (OMB) to begin surveying both covered entities (CEs) and business associates (BAs).

Agency representatives have previously said the survey was the first step in resuming the audit program, which Congress required OCR to create under the 2009 HITECH Act. The program has been delayed due to funding and other issues, including setting up the Web portal through which CEs and BAs will complete the survey, but OCR Director Jocelyn Samuels recently told RPP the agency was “committed” to a “robust” audit program (RPP 4/15, p. 5).

OCR completed a “pilot” audit program two years ago that revealed numerous and sundry compliance failures by nearly all 115 CEs that were included (RPP 3/13, p. 1). (BAs were not audited in the pilot.) CEs and BAs have been fearful of the resumption of the audits, particularly because OCR officials have stated that these new findings, unlike those during the pilot, will form the basis of enforcement action by the agency (RPP 10/14, p. 1).

They’ve also been clamoring for substantive information about the audits, which has not been forthcoming from OCR.

continued on p. 10

New OCR Resolution Agreement Has an Old Ring: Paper Files Are Still a Problem

Paper patient records left unattended have cost a covered entity (CE) a financial payment and a corrective action plan (CAP) with the HHS Office for Civil Rights (OCR). Quick question: in what year did this happen?

A — It just happened – 2015.

B — Maybe it’s 2014, which is when an Indiana health care system paid $800,000 for its actions in dumping 70 boxes of files on the driveway of a physician (RPP 7/14, p. 1).

C — 2011, when Massachusetts General ponied up $1 million for the misdeeds of a worker who left paper scheduling sheets for an HIV clinic on a commuter train (RPP 3/11, p. 1).

D — It could be 2009-2010, when CVS Pharmacy, Inc., paid $2.5 million, and the next year, when Rite Aid Corp., plunked down $1 million to settle allegations related to patient files found in its dumpsters (RPP 8/10, p. 12).

E — All of the above.

The answer: E.

Covered entities, business associates (BAs) and HIPAA advisors can be forgiven if they guessed wrong. The fact is, OCR’s recent announcement of a settlement over paper records — its first resolution of the year, by the way — sounded a tad weary of this problem.

continued
OCR’s undated news “bulletin” posted on its website and the notice to a listserv state “HIPAA Settlement Highlights the Continuing Importance of Secure Disposal of Paper Medical Records.” Both appeared on April 27.

The terms of the new settlement, with Cornell Pharmacy of Denver, a single-location business that specializes in compounded medications, are modest given that OCR contends there was not only improper dumping of protected health information (PHI) on paper files, but also that Cornell lacked policies, procedures and training related to the privacy rule. However, the settlement contains a provision that does not seem to have appeared in other OCR settlements, namely that all workers “report” any possible privacy violations internally “as soon as possible.”

According to OCR, the settlement again sends home the message that paper records need safeguards.

“Regardless of size, organizations cannot abandon protected health information or dispose of it in dumpsters or other containers that are accessible by the public or other unauthorized persons,” OCR Director Jocelyn Samuels said in the bulletin. “Even in our increasingly electronic world, it is critical that policies and procedures be in place for secure disposal of patient information, whether that information is in electronic form or on paper.”

While not admitting wrongdoing, pharmacy owner Tony Jones agreed to a two-year CAP and $125,000 payment. For his part, Jones was definitely not eager to discuss the settlement. “I’ve paid my fine. I’m not making any comments,” he said by phone, before wishing RPP a nice day and hanging up.

TV Station Found the Files

Allegations that the pharmacy mishandled PHI came to light in early 2012 after a local television station checked into a tip it had received that files had been discarded in an unlocked dumpster behind the pharmacy.

According to the resolution agreement, the station contacted OCR on January 11, 2012. Although not mentioned in these documents, the station broadcast a report headlined “Pharmacy Flub” on Feb. 12, 2012. The station showed the reporter discussing the documents with pharmacy members who had come outside, and shortly thereafter transporting the papers to the station while speculating the business could face a “huge federal fine” for leaving the files unsecured.

At the time, the station speculated the PHI for some 5,000 patients had been in the dumpster. According to OCR’s bulletin, the actual number was 1,610.

The station also reported receiving a statement from an attorney for Cornell, who said “failing to shred the document was inadvertent” and that “someone had cut the lock off the dumpster.” Apparently the station gave the documents back to Cornell so that it could notify affected patients.

Then-OCR Director Leon Rodriguez appears on camera during the four-minute segment, saying that, generally speaking, circumstances such as those the station uncovered were “clearly something that we view as a violation, something for which, depending on the circumstances, we might impose significant monetary penalties.” (See the video at http://tinyurl.com/pjcwymv.)

OCR Found No Privacy Policies

According to the settlement, OCR began its investigation on Feb. 27, 2012, two weeks after the TV segment aired, but it would then take more than three years before the agency announced it had reached a resolution agreement. This is still quicker than the five years it took OCR to close the next most recent dumping case. In June 2014, OCR and an Indiana health care network settled for $800,000 and a one-year CAP (RRC 12/14, p. 1).

The incident does not appear on OCR’s “wall of shame,” the website where breaches affecting 500 or more individuals are posted.
OCR, in the settlement documents, said the pharmacy, “[f]rom the compliance date of the Privacy Rule to the present,” had failed to “implement any written policies and procedures as required” nor offered “training on policies and procedures to its workforce as required by the Privacy Rule.”

Oddly, OCR did not mention whether the pharmacy was compliant with the security rule and breach notification regulation. The pharmacy’s website currently contains a notice of privacy practices, dated September 2013, which lists Jones as the privacy officer. It also has a feature called “Ask the pharmacist,” which has an emblem indicating it is a “HIPAA compliant” form for communicating with the pharmacy.

**Agreement Requires Basic Measures**

The resolution agreement, dated April 22, requires the pharmacy to submit proposed policies and procedures to OCR within 30 days. Among the specifics OCR cites that these must address are “[a]dministrative and physical safeguards for the disposal of all non-electronic PHI that appropriately and reasonably safeguard such PHI from any use or disclosure in violation of the Privacy Rule and that limit incidental uses and disclosures, including, but not limited to, providing that paper PHI intended for disposal shall be shredded, burned, pulped, or pulverized so that the PHI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.”

The CAP also contains a few unusual provisions, including the establishment of “internal reporting procedures.”

Specifically, OCR is requiring that Cornell make sure that “all members of its workforce report to the designated Privacy Officer at the earliest possible time, any violation of the Policies and Procedures of which she or he is aware.”

OCR also required that, “upon receiving information that a member of its workforce may have violated these policies and procedures, [Cornell] shall promptly investigate and address the violation in an appropriate and timely manner” and that such workforce members be dealt with.

The CAP calls for Cornell to apply “appropriate sanctions (which may include re-training or other instructive corrective action, depending on the circumstances) against members of [Cornell’s] workforce, including supervisors and managers, who fail to comply with the…Policies and Procedures.”

Once approved by OCR, Cornell must implement the new policies and procedures and train workers on them within 30 days.

**Baptist Healthcare Bans SSNs to Reduce Risk, Please Patients**

As soon as Americans get Social Security cards, they’re told to guard them with their lives, as lost or stolen Social Security numbers (SSNs) raise the stakes for financial fraud and identity theft.

So why, patients started asking Baptist Healthcare, was the South Florida system regularly asking for their SSNs? Why indeed, wondered Baptist officials.

In the hands of criminals, SSNs really are the Holy Grail of protected health information (PHI) and weren’t always necessary for Baptist to have, reasoned administrators at the six-hospital system. Or, perhaps they could severely restrict their use and develop work-arounds to where they might be needed.

And so began a three-year odyssey to scrub SSNs from the hospital system’s electronic records, forms and other documents. The effort has been such a success that it is now at the point where there should be so few numbers in use that Baptist launched a “scavenger hunt,” complete with prizes, to ensure SSNs don’t begin to creep back into use.

Mercy del Rey, Baptist’s chief privacy officer, briefly described getting rid of SSNs during a session with other privacy officers at the recent 23rd National HIPAA Summit in Washington, D.C. (RRC 4/15, p. 1). She also provided additional details to RPP after the meeting.

**Removing SSNs Is ‘Data Cleansing’**

How Baptist went about the process may spur others to undertake similar actions. These may be especially worthwhile in light of increasing data breaches and serve as a relatively inexpensive fix to increase safeguards around PHI. HIPAA consultant John Gomez tells RPP that banning or reducing the use of SSNs is a form of “data cleansing,” a strategy that he recommends.

Del Rey tells RPP the reasons Baptist removed SSNs centered on “patient safety and security.”

“With the increase of identity theft and medical identity theft, patients were questioning why this information [SSNs] appeared in their record,” she says. “Although this was sometimes a technically challenging process for us, we knew [removing them] was the right thing for our patients.”

In July 2013, Baptist announced a breach at one of its medical centers, South Miami Hospital, the result of a theft of more than 800 medical records by a respiratory therapist. During 2011 and 2012, the therapist sold PHI, including SSNs, to two men who filed false tax returns.

“We began removing the SSNs from our system before the 2013 breach,” del Rey tells RPP.

continued
When pressed a little further about whether there was a connection between the SSN removal and the medical records theft, a spokeswoman for the system told RPP by email that “Baptist Health generally doesn’t provide public comment on specific timeframes or other specific details surrounding implementation of compliance projects.”

**Hunting for the ‘Source’**

To get started, Baptist systematically “analyzed our clinical systems to determine where and why [an] SSN was present,” she explains. “A methodical approach was then followed to review all clinical systems to identify the location of the source where SSNs resided in order to ultimately remove it from that system.” If the source of the number isn’t found, it “could potentially reappear in a report or be sent to another system during an interface,” del Rey says.

It took three years to “remove all of the SSNs from all of our clinical systems,” a task del Rey described as “tough.”

“As mentioned during the conference, many of our clinical systems are legacy systems that have been in place for a very long time, so we had to carefully begin our analysis,” she says.

Baptist also recognized that officials couldn’t stop there. “As we have removed SSNs from particular systems or other records, we have provided our staff with additional appropriate training,” del Rey says.

Del Rey also tells RPP that, on top of the “basic HIPAA training that all workforce members receive, we have focused education on areas that have highly sensitive patient information as well as strict role-based security where we constantly re-evaluate the need for that access.”

---

**Congress Orders the Removal of SSNs From Medicare Cards**

Baptist Health of South Florida, a Miami-based system, recently completed a three-year campaign to severely restrict the use of Social Security numbers (SSNs) in its records. Officials said they took these steps, in part, because patients questioned why they were being asked for their numbers.

Yet while Baptist Healthcare patients may have been questioning the system’s use of SSNs, its older ones who are Medicare beneficiaries have been carrying around Medicare cards with their SSNs on them and routinely giving them to their providers to verify eligibility for benefits and to ensure proper billing.

But thanks to the new “Doc Fix” law that repealed the system for setting payment rates for physicians who accept Medicare Part B, covered entities that accept new Medicare patients in the next couple of years may automatically be seeing and accumulating fewer SSNs in their medical records systems.

This legislation requires HHS to remove SSNs from beneficiaries’ cards, out of growing fears of identity theft.

The legislation calls for HHS, by 2018, to “establish cost-effective procedures to ensure that a Social Security account number (or derivative thereof) is not displayed, coded, or embedded on the Medicare card issued for beneficiaries to an individual who is entitled to benefits under part A of title XVIII or enrolled under part B of title XVIII and that any other identifier displayed on such card is not identifiable as a Social Security account number (or derivative thereof).”

Congress also asked HHS to ensure the process “involves the least amount of disruption to, as well as necessary assistance for, Medicare beneficiaries and health care providers, such as a process that provides such beneficiaries with access to assistance through a toll-free telephone number and provides outreach to providers.”

The legislation provides $245 million for HHS to work with on this task.

SSNs became the default way some covered entities (CEs) verified patients’ identities. Providers have their own unique number as created under the administrative provisions of HIPAA.

HIPAA also called for the development and use of a national patient identifier that would be unique to each person. Yet Congress has consistently inserted language in appropriations legislation prohibiting the government from moving forward with this concept, out of concerns that such numbers could actually jeopardize privacy and security.

With the push toward increasing use of patient portals, the movement to get some sort of standard patient identifier that would be unique to each person. Yet Congress has consistently inserted language in appropriations legislation prohibiting the government from moving forward with this concept, out of concerns that such numbers could actually jeopardize privacy and security.

HIMSS has formed an Identity Management Task Force to encourage the government, with HIMSS’ help, to keep moving on the issue. (For more information, see http://tinyurl.com/ph6yhmm.)
Baptist officials, she adds, “also run criminal back- 
ground checks on all employees, which includes those 
members of our workforce who will have access to PHI.”

Perhaps ironically because Social Security numbers 
can be used to commit identity theft, del Rey says “[one 
of the biggest] challenges we faced involved the use of 
the SSNs to assist with the accurate identification of a 
patient.”

Del Rey points out that “many patients in our service 
areas have the same name with similar demographics so 
in the past we relied on the SSNs as one of the identifiers. 
Once we made these changes, our processes focused 
on other demographics and the use of only the last four 
digits in those cases where patients shared similar demo-
graphic data.”

Not all uses can be eliminated. For example, when 
they appear “in billing systems where the Medicare 
identification number is the individual’s SSN, [Baptist 
officials] restrict access and have provided staff that do 
need access with additional training on safeguards and 
sensitivities regarding the use of SSNs,” del Rey says.

The government has made little progress in develop-
ing a unique patient identifier; calls for this have been 
renewed. Congress recently told HHS to remove SSNs 
from Medicare cards (see box, p. 4).

During the summit discussion, del Rey stressed the 
value of positive reinforcement as a form of workforce 
training. When it comes to the SSN issue, Baptist devel-
oped a special contest, or a scavenger hunt, under which 
employees call del Rey’s office if they find an SSN, for 
which they receive a special gift — a tiny cup used for 
Cuban coffee.

Scavenger Hunt Is a Win-Win

“We have had employees find them through our 
scavenger hunt,” del Rey reports. “This is a win-win 
scenario for our patients, our employees and our or-
ganization. Our patients’ information is further secured, 
our employees are actively engaged in our compliance 
activities and are recognized for their efforts and finally 
our commitment to protecting our patients’ information 
is reinforced throughout the organization.”

John Gomez, former chief technology officer at 
Allscripts Healthcare Solutions and WebMD, tells RPP 
that removing SSNs and other sensitive data — espe-
cially if it’s not needed — is a good compliance strategy. 
Gomez, founder and CEO of the cybersecurity firm Sen-
sato, Inc., says this is a type of “data cleansing.”

Gomez adds that even though it took Baptist three 
years to do this, “it’s probably a cheap thing to do” and is 
among the more basic strategies that CEs can undertake 
without costly IT investments.

He also likes the idea of getting all staff involved in 
searching for SSNs. Such programs, he says, make it clear 
for the workforce that “this is our data. We own all that” 
and spreads the sense that each worker has a responsibil-
ity to safeguard the PHI.

As Baptist’s experience shows, removing the SSNs 
and keeping them from creeping back in takes a redesign 
of paper forms, a blocking of data fields that ask for them 
and other IT fixes. It also takes a concerted effort to stop 
staffers from creating new forms as well as adding new 
software or programs that ask for them.

As del Rey says, “It’s important to note that this re-
view, though, really never ends. When any new system is 
being implemented, the use of the SSNs is assessed and 
evaluated as part of our routine reviews.”

Contact del Rey at MercyDR@baptisthealth.net and 
Gomez at john.gomez@sensato.com.

New Ponemon Report: Covered Entities Lack Resources, Staff

During a recent two-year period, 59% of business 
associates (BAs) reported having a data breach, a costly 
fate suffered by 91% of covered entities (CEs), according 
to the Ponemon Institute’s Fifth Annual Benchmark Study 
on Privacy & Security of Healthcare Data.

Issued May 7, the new report reflects the responses 
of 90 CEs and 88 BAs, and marks the first time business 
associates have been included. For that reason alone — 
and there are many others — the new report demands a 
look. But with so many CE’s complaining that their BAs 
are not HIPAA-compliant and so many BAs listed on the 
HHS Office for Civil Rights’ data breach wall of shame, 
is it really possible that BAs are doing a better job than 
CEs, and that CEs are suffering twice as many breaches 
as BAs?

Well, maybe not.

In an interview with RPP, Larry Ponemon, chairman 
and founder of the Ponemon Institute, says that BA data 
really need to be taken with a grain of salt. “I consider 
it [the number of breaches by BAs] an under-report,” 
Ponemon tells RPP in an interview. For one thing, BAs, 
he says, are “not as sophisticated in identifying data leak-
age” as CEs are.

To look at it another way, the fact that 59% of BAs 
have suffered at least one breach, which isn’t exactly a 
perfect record, may be eye-opening to some CEs whose 
BAs might never have reported having any breaches to 
them.

When business associates were asked to list what 
best describes their organization, 35% said pharmaceutical 
firms; 21% IT services/cloud services; 19% data/
claims processor; and 15% transcription or other medical-related services.

Of those that had breaches, 30% of BAs said they’d had only one, compared to 12% of CEs. More commonly, however, the data showed 39% of CEs and 14% of BAs had two to five breaches; and 40% of CEs and 15% of BAs had five or more, according to the report, which is sponsored by ID Experts.

Comparing the five-year Ponemon data that are available for CEs only, the number of breaches has risen since 2010 but not in every year, as follows:

- In 2010, 26% of covered entities had one breach, 31% had two to five, and 29% had more than five.
- In 2011, 4% had none, 17% had one, 33 had two to five, and 46% had more than five.
- In 2012, 6% had none, 16% had one, 33% had two to five, and 45% more than five.
- In 2013, 10% had none, 16% had one, 36% had two to five, and 38% more than five.

What’s behind the breaches? One challenge, says the report, is there are a “variety of root causes.” Organizations were permitted to list more than one cause of their breaches. This is the first year that criminal attacks rose to the top of the list, overtaking lost or stolen computing devices.

- 45% of CEs and 39% of BAs say they suffered a criminal attack;
- 43% of CEs and 35% of BAs say the cause was a lost or stolen computing device;
- 40% of CEs and 51% of BAs cite an “unintentional employee action”; and
- 39% of CEs and 49% of BAs attribute their loss to a “third-party snafu.”

Some of the findings also show a mismatch of causes and organizational attention. For example, “web-borne malware attacks caused security incidents for 78 percent of healthcare organization and 82 percent of BAs. Despite the changing threat environment, however, organizations are not changing their behavior — only 40 percent of

<table>
<thead>
<tr>
<th>Security incidents healthcare organizations experienced</th>
</tr>
</thead>
<tbody>
<tr>
<td>(More than one response permitted)</td>
</tr>
<tr>
<td>Lost or stolen devices</td>
</tr>
<tr>
<td>Spear phishing</td>
</tr>
<tr>
<td>Web-borne malware attacks</td>
</tr>
<tr>
<td>Exploit of existing software vulnerability greater than 3 months old</td>
</tr>
<tr>
<td>Exploit of existing software vulnerability less than 3 months old</td>
</tr>
<tr>
<td>SQL injection</td>
</tr>
<tr>
<td>Advanced persistent threats (APT) / targeted attacks</td>
</tr>
<tr>
<td>Spyware</td>
</tr>
<tr>
<td>DDoS</td>
</tr>
<tr>
<td>Zero day attacks</td>
</tr>
<tr>
<td>Botnet attacks</td>
</tr>
<tr>
<td>Clickjacking</td>
</tr>
<tr>
<td>Rootkits</td>
</tr>
<tr>
<td>Other</td>
</tr>
</tbody>
</table>

SOURCE: Ponemon Institute’s Fifth Annual Benchmark Study on Privacy & Security of Health Data

Copyright © 2015 by Atlantic Information Services, Inc. All rights reserved.
Please see the box on page 2 for permitted and prohibited uses of Report on Patient Privacy content.
healthcare organizations and 35 percent of BAs are concerned about cyber attackers,” the report states.

Answers to questions about how prepared both CEs and BAs are to handle threats to their security are illuminating. For example, fully 35% of CEs and BAs were “unsure” whether their organization “has sufficient resources to prevent or quickly detect unauthorized patient data access, loss or theft.” Only 23% of CEs and 21% of BAs said they “strongly agree” with the statement that the organization has “personnel who have technical expertise to identify and resolve the authorized access, loss or theft.”

Asked if there is a shortage of such personnel or whether the issue is not enough money being spent to hire them, Ponemon says both are factors. He says research indicates 60% of IT positions are “vacant,” and that the U.S. simply isn’t producing enough individuals with the “deep knowledge” and skills to fill these posts.

Additionally, however, many health care entities think paying $120,000 a year “for an IT person” is too high and will aim to spend half of that or slightly higher, Ponemon says, so they are not attracting the people they really need.

“What we have seen, in general, is a lot of people who do security are not,” he says, “expert in security.”

Lost or stolen devices were by far the most common types of “incidents” to occur for both CEs and BAs (96% and 95% respectively); spear phishing, at 88% and 90% respectively, was second. Respondents could list more than one type.

Several questions about clouds revealed interesting data. Eighty percent of CEs and 89% of BAs reported they were “moderate” or “heavy” users of clouds, with just 5% of CEs and zero BAs saying they didn’t use clouds at all.

Sixty percent of CEs and 45% of BAs said email was one type of information they process or store in a “public cloud environment.” Approximately 50% of both CEs and BAs use clouds for “employee information including payroll data,” and 50% of CEs and 39% of BAs also make use of clouds for “accounting and financial information.”

Approximately 35% of both groups also use clouds for “patient medical records” and “patient billing information.” Yet in response to the question “What types of information does your organization consider too sensitive to be processed and/or stored in a public cloud environment,” 50% of CEs and 44% of BAs said patient medical records.

The most common cloud-based “applications” were “business applications (such as Salesforce.com, webmail, HR, etc.),” with 56% for CEs and 63% for BAs reported; and second was for “back up and storage,” with CEs at 49% and BAs at 48%.

What security threats healthcare organizations worry about most
(Three responses permitted)

<table>
<thead>
<tr>
<th>Threat</th>
<th>CE Percentage</th>
<th>BA Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee negligence</td>
<td>70%</td>
<td>70%</td>
</tr>
<tr>
<td>Cyber attackers</td>
<td>40%</td>
<td>40%</td>
</tr>
<tr>
<td>Use of public cloud services</td>
<td>33%</td>
<td>33%</td>
</tr>
<tr>
<td>Mobile device insecurity</td>
<td>32%</td>
<td>32%</td>
</tr>
<tr>
<td>Employee-owned mobile devices or BYOD</td>
<td>29%</td>
<td>29%</td>
</tr>
<tr>
<td>Malicious insiders</td>
<td>26%</td>
<td>26%</td>
</tr>
<tr>
<td>Identity thieves</td>
<td>19%</td>
<td>19%</td>
</tr>
<tr>
<td>Process failures</td>
<td>15%</td>
<td>15%</td>
</tr>
<tr>
<td>System failures</td>
<td>15%</td>
<td>15%</td>
</tr>
<tr>
<td>Insecure mobile apps (eHealth)</td>
<td>13%</td>
<td>13%</td>
</tr>
<tr>
<td>Insecure medical devices</td>
<td>6%</td>
<td>6%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
<td>2%</td>
</tr>
</tbody>
</table>

Source: Ponemon Institute’s Fifth Annual Benchmark Study on Privacy & Security of Health Data
OCR Offers Guidance, EEOC Explains HIPAA and Workplace Wellness

In late April the Office for Civil Rights posted two new questions and answers addressing HIPAA privacy and security and workplace wellness programs. These appeared in conjunction with the publication of a proposed rule by the Equal Employment Opportunity Commission (EEOC) addressing the intersection of the nondiscrimination provisions of the Americans With Disabilities Act (ADA) and HIPAA in wellness programs, as well as the confidentiality of any medical information gathered for these programs.

The OCR Q&A points out that HIPAA applies only to covered entities and their business associates, and as a general rule, employers are not covered entities in their capacity as employers. However, if an employer offers a workplace wellness program as a benefit of its group health plan, the health information collected is PHI that is subject to HIPAA protections, because the group health plan is a covered entity. If the employer offers a wellness program that is not part of the group health plan, the health information is not protected by HIPAA.

If the employer/plan sponsor does not administer its plan, then the group health plan may disclose only the following to the employer:

“(1) Information on which individuals are participating in the group health plan or enrolled in the health insurance issuer or HMO offered by the plan; and/or

“(2) Summary health information if requested for purposes of modifying the plan or obtaining premium bids for coverage under the plan.”

Employers that administer their own group health plan may receive additional PHI subject to certain conditions. According to the OCR Q&A, “the group health plan may provide the employer as plan sponsor with access to the PHI necessary to perform its plan administration functions, but only if the employer as plan sponsor amends the plan documents and certifies to the group health plan that it agrees to, among other things:

♦ “Establish adequate separation between employees who perform plan administration functions and those who do not;

♦ “Not use or disclose PHI for employment-related actions or other purposes not permitted by the Privacy Rule;

♦ “Where electronic PHI is involved, implement reasonable and appropriate administrative, technical, and physical safeguards to protect the information, including by ensuring that there are firewalls or other security measures in place to support the required separation between plan administration and employment functions; and

♦ “Report to the group health plan any unauthorized use or disclosure, or other security incident, of which it becomes aware.”

See 45 CFR §164.314(b) and §§164.504(f)(1)(i) and (f)(2); visit http://tinyurl.com/ok37e9y for the Q&As.

EEOC Regs Rely on HIPAA for Confidentiality

The Equal Employment Opportunity Commission on April 20 published a proposed rule to amend regulations implementing the ADA with regard to wellness programs. Specifically, the guidance discusses the extent to which employers may use incentives to encourage employees to participate in wellness programs that include disability-related inquiries and/or medical examinations. Title I of the ADA restricts the medical information an employer may obtain from an individual and makes it illegal to discriminate based on disability. And here’s where HIPAA comes into play.

The proposed rule discusses the nondiscrimination provisions of the ADA as they relate to the nondiscrimination provisions of HIPAA, which are in a separate title from the privacy and security provisions. But it also addresses how employers must protect any information gathered from employees with regard to participation in the wellness programs to comply with the HIPAA privacy regulations. As proposed, the EEOC would add a new subsection (6) to 29 CFR §1630(d), which states that “medical information collected through an employee health program only may be provided to a covered entity under the ADA in aggregate terms that do not disclose or are not reasonably likely to disclose, the identity of specific individuals,” except as needed to administer the plan or if permitted under 29 CFR §1630(d)(4). That section permits disclosure to supervisors and managers regarding necessary restrictions on the work or duties of the employee and necessary accommodations, first aid and safety personnel if the disability might require emergency treatment; and government officials investigating compliance with the ADA regulations.
If an employer does not administer its group health plan, then any PHI it receives must be de-identified as prescribed in HIPAA.

The preamble states that a wellness program that is part of a group health plan, which is a covered entity, generally will be in compliance with the new ADA provision if it complies with all of HIPAA’s privacy rules for use and disclosure. Thus, certain disclosures that may be permitted under 29 CFR §1630.14(d)(4) for employee health programs may not be permissible without an individual’s authorization because of the privacy rule.

Visit http://tinyurl.com/kvya7kl for the text of the rule.

Poll: Breaches, Not Compliance, Now Drive Health Care IT Spending

Another industry survey on the state of health care’s ability to protect its data has reached an overall conclusion that is similar to the other surveys that have been released over the last several months — health care IT is behind other industries, and “the results clearly point to systemic failures...when it comes to protecting sensitive data.”

The new survey was conducted by Harris Poll on behalf of Vormetric, which describes itself as “the industry leader in data security solutions that protect data-at-rest across physical, big data and cloud environments.” U.S. health care IT decision makers from 102 organizations with at least $200 million in revenue responded, so clearly the survey’s focus was on the larger health care organizations. It is not surprising, therefore, that the two biggest risks identified by the respondents were the cloud and Big Data (massive amounts of data that are too large to be processed on standard computers using traditional database programs and software). And when Big Data is stored on the cloud, the vulnerability increases exponentially.

‘Privileged Users’ = Risk

But the survey includes some other interesting data points on the “most dangerous” insiders, why organizations secure data and how they allocate spending.

Many surveys point a finger at “employees” in general as the biggest insider threat to data security. Vormetric dives in a little deeper and says that “privileged users,” who traditionally have access to all resources available from systems that they manage and credentials for their accounts, were identified as the most dangerous inside threat (62%). This was illustrated by the Anthem, Inc. breach where a privileged user account was the entry point. Partners with internal access to the systems (46%) and contractor/service-provider employees (45%) came in second and third respectively.

Prior to this 2015 survey, respondents identified “compliance” as the primary driver for data security. Now, compliance remains the primary reason why health care organizations secure their data (54%), but data breaches are the primary driver behind IT spending (53%) and are in third place when it comes to reasons for securing the data (40%). According to the survey, “this supports the conclusion that healthcare organizations have not fully absorbed the need to change their priority set.”

The survey also found that health care organizations are planning the largest investment in data-at-rest defenses and analysis/correlation tools with slightly lower levels planned for data-in-motion, end-point and mobile and network defenses. Respondents also reported that they believe these tools are effective 83% of the time in preventing insider threats. Fifty-eight percent believe that compliance requirements are “very” or “extremely” effective at neutralizing insider threats.

“Organizations are still heavily investing in traditional perimeter defenses, which are not effective at stopping the new generation of threats facing the healthcare vertical.” Compliance requirements now are more of a good baseline from which to build more effective data security, but not sufficient to protect organizations against current threats.

New Data Strategies Are Needed

“What is needed,” the survey concludes, “is a data-first security strategy.” It sets out five points for health care organizations to implement this strategy:

◆ “With network and endpoint security solutions failing to stop or even detect attacks by employee insiders, and advanced attacks using employee credentials, a layered defense combining traditional as well as advanced data protection techniques is the path forward.

◆ “Data protection initiatives need to concentrate on protecting data at the source. For most organizations, this will involve protecting a mix of on-premise databases and servers, and remote cloud and Big Data applications.

AIS’s Management Insight Series
Best Practices to Make Your Physician Contracts Stark Compliant

Go to the “Marketplace” at www.AISHealth.com and click on “Books, Insight Series.”

---

Subscribers who have not yet signed up for Web access — with searchable newsletter archives, Hot Topics, Recent Stories and more — should click the blue “Login” button at www.AISHealth.com, then follow the “Forgot your password?” link to receive further instructions.
“Companies should integrate new encryption technology that minimizes operational impact and works with strong access controls for all important data sources.

“Implementing integrated data monitoring and technologies such as security information and event management (SIEM) systems to identify data usage and unusual and malicious access patterns is critical to maximizing security.

“To keep the whole organization safe, companies must develop an integrated data security strategy that includes monitoring, relevant access control and levels of data protection — and leaves security to the CISO, not the boardroom.”

Visit http://tinyurl.com/nue5gxm and scroll down to “healthcare” under “Major Markets and Verticals.”

OMB Approved OCR’s Audit Survey

As the survey explains, “This screening questionnaire is intended to gather data about the size, complexity, and operations of potential audittees for the HIPAA Privacy, Security and Breach Notification Audit Program. These data will be used with other information to help us select entities that reflect a variety of types, size, and locations for the Audit Program. Please note that if your organization is selected for audit, communications from OCR will be sent to the email addresses of the contact persons identified [on the questionnaire].”

In February 2014, OCR published a request for comments about the survey in the Federal Register (RPP 3/14, p. 1). OCR then submitted the screening tool to OMB for approval on May 19, 2014, according to reginfo.gov, the federal website where regulations and other government activities are posted. OMB “approved with change” OCR’s “pre-audit screening tool” on March 13.

Approval Took a Long Time

It is not clear what the change was or why it took so long to pass muster with OMB. As posted on the reginfo.gov website, the survey is a straightforward and basic request for simple information.

According to the posting on reginfo.gov, OMB granted OCR’s request to survey 500 CEs and 200 BAs. In addition to posting the survey, OMB also linked to the agency’s “justification” for conducting it, a normal part of government operations when a regulation, or an information request as is this survey, is planned.

The survey has a total of 37 questions, broken out into sections for different types of CEs — providers, health plans and clearinghouses — and one for business associates. All organizations are asked to specify financial information, including “total revenue for the most recent fiscal year.”

OCR estimated it would take CEs and BAs only 30 minutes to complete the questionnaire. “Respondents will respond to the data collection one-time only for a given round of OCR audits. OCR makes efforts to not duplicate audits for prior audited covered entities, meaning that OCR would not send a pre-audit screening questionnaire to an entity that was audited in recent years,” the justification document states. “However, an entity may be asked to respond to a pre-audit screening questionnaire during a subsequent round of OCR audits.”

Although none would qualify as “gotcha” questions that might trick an entity into revealing some possible area of noncompliance, a few are noteworthy.

Two questions in the health plan section deal with “sponsors.” One asks, “If you are a health plan, are you a group health plan sponsor responding on its behalf?” Another is, “If you are a group health plan sponsor, do you receive only summary data from the group health plan, health insurer (sic) issuer, or HMO?”

One question of note for clearinghouses: “Do you operate only as a business associate and do not maintain protected health information or perform covered functions as a covered entity apart from your activities as a business associate?”

BA s Are a Challenge for OCR

OCR officials have previously acknowledged that cracking the business associate market is a challenge for them. BAs are numerous and not always readily identifiable; some have refused to acknowledge their status as a BA, at least until recently.

Questions for BAs ask them to “briefly describe the nature of your business associate activities (e.g., billing, third party administrator, information technology support, legal services, etc.),” as well as the “number and type” of each of these.

Another survey question states, “Identify whether any of the covered entity(ies) for which you provide business associate functions are Organized Health Care Arrangements (OHCA) or Affiliated Covered Entities (ACE) (choose all that apply).” One of the options for answering is “not sure.”

OCR also asks business associates, “What is the total revenue from all of your business associate activities in the most recent fiscal year?,” a question that implies OCR understands that some organizations have lines of business that don’t cross over into HIPAA territory.

To date, OCR officials, including Samuels, have not mentioned obtaining approval of the survey when they’ve recently spoken at public meetings. Now that the survey has been approved, RPP asked OCR whether it
has already begun contacting the CEs and BAs that will be asked to complete it.

RPP also asked other related questions, such as when the protocol for the audits would be published and whether there would be a different one for CEs and BAs.

Covered entities are eager to see the protocol so they can use it to prepare for the possibility they may be audited. In the meantime, some say they can do little more than review their policies and procedures and ensure they have a list of all their business associates, which OCR has said it will request of the CEs it selects for the audit (RPP 4/15, p. 1).

But it seems that the audit program is in flux, as agency spokeswoman Rachel Seeger said in an email to RPP: “At this time, OCR cannot speak to your questions concerning the details of the audit program, including the timing and scope of the survey. Further, we cannot offer details to you at this time on other aspects of this program. Announcements regarding the program will be made on the OCR web site and listserv.”

PRIVACY BRIEFS

◆ Partners Healthcare is the latest health system to fall prey to an email phishing attack, which compromised the records of 3,300 patients, it said on April 30. The scam, which Partners uncovered on November 25, 2014, resulted in several employees giving out account access information. Partners said the attackers were not able to compromise its database, and gained access only to information contained in the breached email accounts. That information included names, dates of birth, phone numbers, addresses, medical diagnoses, treatments, medical record numbers, insurance information and Social Security numbers. Visit http://tinyurl.com/q5shzu9.

◆ Email phishing resulted in the breach of information for 39,000 patients of Seton Family of Hospitals, the health system said on April 24. The attack occurred in December 2014, and Seton determined in February 2015 the compromised accounts contained names, dates of birth, addresses, gender, medical record numbers, insurance information, some clinical information and Social Security numbers. Visit http://tinyurl.com/198j6mp.

◆ A stolen laptop potentially exposed the PHI of an undisclosed number of members of Oregon’s Health CO-OP, the health plan said on April 28. The CO-OP also mixed up addresses while mailing letters to affected individuals, resulting in a second breach. While the CO-OP said it had no reason to believe the compromised information has been misused since the theft on April 3, it also did not specify whether the information had been encrypted. The laptop contained names, dates of birth, addresses, health plan numbers, ID numbers and Social Security numbers. Visit http://tinyurl.com/nddevmq.

◆ An email phishing scam potentially compromised the information of 25,000 patients of Baltimore-based Saint Agnes Hospital, the hospital said on April 27. “Sophisticated hackers” stole a user name and password to an employee’s account, which the hospital said it immediately shut down upon discovery. Potentially compromised information included names, dates of birth, gender, medical record numbers, insurance and clinical information and, for four patients, Social Security numbers. The hospital did not provide details on when the attack occurred or how long the investigation took. Visit http://tinyurl.com/puq45kx.

◆ The National Association of Insurance Commissioners on April 16 officially adopted new guidelines regarding cybersecurity and patient privacy. The guidelines detail eight principles governing insurance commissioners’ responsibilities in the defense of protected health information, including conducting risk reviews, establishing incident response procedures, verifying third-party security controls and collaborating with insurers to develop regulations. Visit http://tinyurl.com/oaaw8w9h.

◆ The PHI of nearly 3,000 patients at Arlington Heights, Ill.-based Suburban Lung Associates was exposed after a vendor left documents unattended prior to their destruction, the clinic reported to the Office for Civil Rights on April 13. The vendor was scheduled to destroy the documents, which concerned patients who last visited the clinic in 2004. Potentially breached information included names, dates of birth, addresses, phone numbers, diagnoses, treatment information and Social Security numbers. Visit http://tinyurl.com/q3dtovg.

◆ Zero-day vulnerability attacks, or hacks executed on vulnerable points in a software program that are unknown to the vendor, reached an all-time high of 24 in 2014, according to Symantec Corp.’s April 14 cybersecurity report. The 2015 In-
PRIVACY BRIEFS

The San Francisco Chronicle announced on April 6 that hackers are moving faster and improving their strategies much more quickly than companies are. For the top three zero-day attacks, it took 204 days, 22 days and 53 days for vendors to design a patch; the average time in 2013 was four days. Visit http://tinyurl.com/k276deg.

◆ More than 29 million patient records were compromised between 2010 and 2013, according to a study published April 14 by the Journal of American Medical Association. Two-thirds of those data were electronic. Three-fifths of the breaches were a result of theft, and 10% were thanks to hackers. The authors concluded some victims may have had their PHI compromised multiple times. Visit http://tinyurl.com/lrvy59g.

◆ Mobile devices are largely exempt from malware attacks, according to the Verizon 2015 Data Breach Investigations Report released on April 13. Of those on the Verizon network, a mere 0.03% were infected with malware each week, and 0.68% of mobile devices were infected overall. In the report, FireEye said 96% of malware was directed at Android devices, and that more than 5 billion Android apps are vulnerable to attacks. However, hackers were able to game Apple’s platform by “hijacking” its beta testing process. Visit http://tinyurl.com/p25eo44.

◆ The Office of the National Coordinator for Health Information Technology (ONC) on April 13 issued a revised version of its Guide to Privacy and Security of Electronic Health Information. The guide is meant to aid HIPAA-covered entities and other health care providers in integrating federal privacy regulations into their business policies. Visit http://tinyurl.com/c66hrp9.

◆ A federal judge dismissed a class action lawsuit against Horizon Healthcare Services over a stolen laptop containing PHI of more than 839,000 Horizon Blue Cross Blue Shield of New Jersey members, according to a document published April 13 by Courthouse News Service. The judge said none of the defendants had demonstrated any injury stemming from the November 2013 theft and, as such, had no grounds to sue. Visit http://tinyurl.com/m7ffpdd.

◆ A former respiratory therapist at Oregon, Ohio-based Bay Park Hospital has been indicted on HIPAA-related charges for allegedly inappropriately accessing patient information between May 2013 and March 2014, NBC24 reported on April 6. The police had previously declined to bring charges in June 2014 due to a lack of evidence, but now believe they have sufficient cause for prosecution. Visit http://tinyurl.com/k49ggbt.

◆ Seven out of 10 patients would switch providers after a data breach, according to a recent report from TransUnion Healthcare. But that statistic is largely age-dependent, as 64% of respondents aged 55 and older were unlikely to consider switching, while 73% of participants aged 18 to 34 said they would consider finding a new provider. Visit http://tinyurl.com/kpdt75b.

◆ HITRUST Alliance LLC is conducting an empirical and comprehensive study to evaluate health care cybersecurity threats. The HITRUST Cyber Discovery study will examine methods, pervasiveness and severity of current cyber threats. HITRUST said the end goal is to be able to identify patterns and analyze the sophistication of specific threats. HITRUST will provide resources to the more than 200 health plans that will be participating in the project. Visit https://hitrustalliance.net/cyber-discovery/.

◆ Cybersecurity firm Bitglass on April 7 published the results of an experiment it conducted in January to track where stolen data travels once a system has been breached. The firm concocted a fake list of information such as names, addresses, phone numbers, credit card numbers and Social Security numbers to post on the Dark Web, a vast realm on the internet where hackers and others operate in total anonymity. The list, which Bitglass promoted through phishing and which was downloaded from a proxy service, contained watermarks that pinged Bitglass every time the data were accessed. After a few days, the information had traveled to five countries and three continents and been accessed 200 times. By the 12th day, it had reached 22 countries and five continents and been viewed 1,081 times. The most common points of access were in Brazil, China and Russia, countries known for their high level of cybercrime activities. The findings are especially significant considering the fact that data breaches average 205 days before they are discovered, Bitglass said, and that 53% of breaches are a result of hacking. Visit http://tinyurl.com/qzxlk8h.
IF YOU DON’T ALREADY SUBSCRIBE TO THE NEWSLETTER, HERE ARE THREE EASY WAYS TO SIGN UP:

1. Return to any Web page that linked you to this issue

2. Go to the MarketPlace at www.AISHealth.com and click on “Newsletters.”

3. Call Customer Service at 800-521-4323

If you are a subscriber and want to provide regular access to the newsletter — and other subscriber-only resources at AISHealth.com — to others in your organization:

Call Customer Service at 800-521-4323 to discuss AIS’s very reasonable rates for your on-site distribution of each issue. (Please don’t forward these PDF editions without prior authorization from AIS, since strict copyright restrictions apply.)