Report on
Patient Privacy

Volume 17, Number 8 • August 2017

Practical News and Strategies for Complying With HIPAA

Contents

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

Editor
Theresa Defino
theresa.defino@hcca-info.org

Senior Writer
Jane Anderson

Copy Editor
Nancy Gordon
nancy.gordon@hcca-info.org

Take a Tip From the Former U.S. CISO: 'Harden' Your Workforce to Reduce Risk

When Gregory Touhill was appointed the first chief information security officer (CISO) for the federal government, he devised "five strategic lines of effort" to guard the nation's data. The first and most important of the five: "Hardening the workforce."

"Hardening the workforce harkens back to my time in the military but it also is related to our national cybersecurity framework," says Touhill, referring to the guidelines developed by the National Institutes of Standards and Technology (NIST), part of the Department of Commerce.

Touhill recently testified before Congress on strategies to improve the security of data following the outbreak of malware known as "WannaCry" *(RPP 7/17, p. 1).* Now president of the federal group at the IT security and datacenter firm Cyxtera, Inc., Touhill expounded upon his testimony in an interview with *RPP.*

His tenure as America's first CISO lasted just four months—Touhill was appointed by President Obama in September and served until President Trump took the oath of office in January. No replacement for Touhill has yet been named. But Touhill, who is also a retired brigadier general, arrived at that position after serving as the deputy assistant secretary for cybersecurity and communications in the Department of Homeland Security, among other security-related posts through his career.

continued on p. 10

OCR to Start Over with Long-Awaited Accounting of Disclosures Regulation

The HHS Office for Civil Rights (OCR) plans to scrap its controversial 2011 notice of proposed rule making (NPRM) implementing the accounting of disclosures provisions contained in the 2009 HITECH Act. Instead, OCR will go back to the drawing board to draft a new rule to inform patients who have accessed their protected health information (PHI), says Deven McGraw, the agency's deputy director for health information privacy.

The HITECH Act amended the privacy rule to expand an individual's right to receive an accounting of disclosures of PHI from HIPAA covered entities (CEs) and business associates (BAs). The law requires the accounting to include PHI specifically used to "carry out treatment, payment, and health care operations (TPO) if such disclosures are through an electronic health record."

This provision in the law was a compromise with those who wanted Congress to mandate patient authorization for TPO disclosures, which don't require patient consent, as they are considered essential to health care delivery. CEs state in their notices of privacy practices that such activities will be occurring. In contrast, providers have to obtain a signed authorization to use PHI for marketing purposes, for example.

Under the law, the regulation for the accounting of disclosures was supposed to be issued by June 2010, so by the time OCR completes a new proposed rule it will be nearly a decade past the deadline given by Congress.

continued

McGraw addressed the accounting of disclosures rule during a July 27 webinar on engineering and cybersecurity for connected devices sponsored by the BioPharma Research Council. Webinar host Rebecca Herold, president of the HIPAA consulting firm Simbus360 and CEO of Privacy Professor, asked McGraw what regulations might be forthcoming from OCR, including how it planned to follow up on the 2011 accounting of disclosures NPRM. Her comments appear to mark the first time OCR has publicly acknowledged it is abandoning the 2011 proposed rule.

"We do not have plans to finalize that NPRM," McGraw said. "However, it remains a requirement that we have to fulfill…we have to find some way of enabling individuals to receive accounting of disclosures [for TPO] from an electronic health record as defined in HITECH."

OCR, McGraw says, is "going to need some additional public input on how we can implement this, given that what we had initially proposed was not feasible."

The agency, McGraw says, is "hoping that folks will give us some good ideas through a public comment process, such as an advance notice of proposed rule making" (ANPRM).

Report on Patient Privacy (ISSN: 1539-6487) is published 12 times a year by Health Care Compliance Association, 6500 Barrie Road, Suite 250, Minneapolis, MN 55435. 888.580.8373, www.hcca-info.org.

Editor: Theresa Defino

Subscriptions to *RPP* include free electronic delivery in addition to the print copy, e-Alerts when timely news breaks, and extensive subscriber-only services at www.hcca-info.org that include a searchable database of *RPP* content and archives of past issues.

To order an annual subscription to **Report on Patient Privacy** ($554 bill me; $524 prepaid), call 800-521-4323 (major credit cards accepted) or order online at www.hcca-info.org.

Subscribers to *RPP* can receive 12 Continuing Education Credits per year, toward certification by the Compliance Certification Board. Contact CCB at 888-580-8373.

She did not say when OCR would be doing this outreach, but said it was "coming," perhaps by the end of this year.

If OCR chooses to write an ANPRM, that will be a break from how it wrote its original NPRM. In 2010, a year before issuing the NPRM, OCR issued a formal request for information (RFI), which, like an ANPRM, seeks input but in a less comprehensive manner. At that time, OCR posed nine questions and gave stakeholders just 15 days to submit responses.

An ANPRM will pose questions, as well as challenges, but also offer potential answers or solutions. Comment periods are typically 30 to 60 days.

The change provided for in the HITECH Act greatly expanded CEs' and BAs' responsibilities when it came to informing patients about use of data, and they have been dreading the day it goes into effect. That was evident in their comments when OCR issued a request for information in May 2010 about how it could implement this requirement *(RPP 6/10, p. 1).*

Backlash Greeted Proposed Rule

Before the HITECH Act, patients could request an accounting of disclosures, which would include "(1) The date of the disclosure; (2) the name (and address, if known) of the entity or person who received the protected health information; (3) a brief description of the information disclosed; and (4) a brief statement of the purpose of the disclosure (or a copy of the written request for the disclosure). For multiple disclosures to the same person for the same purpose, the accounting is only required to include: (1) For the first disclosure, a full accounting, with the elements described above; (2) the frequency, periodicity, or number of disclosures made during the accounting period; and (3) the date of the last such disclosure made during the accounting period."

The privacy rule required the disclosures to go back seven years and excluded TPO, but the HITECH removed that if the TPO was disclosed "through an electronic health record." As OCR explained in the 2010 RFI, "under section 13405(c), an individual has a right to receive an accounting of such disclosures that covers disclosures made during the three years prior to the request. Section 13400 of the statute defines 'electronic health record' as 'an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.'"

OCR's 2011 proposed rule on the accounting of disclosures requirement generated a significant backlash, mostly because OCR added a new mandate for a second, new list of disclosures to be contained in what it called an "access report" *(RPP 6/11, p. 1).*

The access report would reveal which workforce members had reviewed PHI contained in a designated record set within the previous three years—a timeline it also set for a regular accounting of disclosures. The proposed rule was called "horrendous" overall. Critics decried the access report as unnecessary and onerous, as few patients had ever exercised the right to obtain an accounting of disclosures under the existing rule.

To meet deadlines for responding to requests, CEs also believed they would have to create access reports in advance, which they said was impossible based on software limitations in electronic health records.

OCR has issued nothing on this topic since the proposed rule, although there has been a lot of discussion. In 2013, a policy committee of the HHS Office of the National Coordinator for Health Information Technology—which McGraw as a private citizen sat on at the time—recommended that HHS pilot test technology to see if reports could be generated as required under OCR's proposed rule.

The committee also recommended OCR require a "report of external disclosures," which it believed would get more to the heart of what patients really want to know about how their PHI is used, and to inform patients of their "right to an investigation of accesses inside the entity" *(RPP 12/13, p. 1).*

For the last couple of years, agency officials have been saying they were working on a final rule *(RPP 10/14, p. 7).* But the regulation was eventually moved to a category of "current long term actions" on reginfo.gov, the website of regulations under development maintained by the Office of Management and Budget. Under the final update President Obama issued in the fall of last year, the issuance date was "to be determined."

However, a new, updated regulatory list published under President Trump in July confirms what McGraw said. It lists the date of the 2011 NPRM and indicates the next step is an ANPRM. But the expected data is listed as November 2018.

ANPRM for Sharing Penalties To Be Issued

The accounting of disclosures regulation isn't the only unfinished task in the HITECH Act that OCR will be working on. McGraw said during the webinar OCR also plans to issue a separate ANPRM to help it write a regulation under which it would share financial penalties collected from CEs and BAs with patients and others affected by HIPAA violations and breaches.

Unlike the accounting regulation, OCR hasn't published anything related to this yet, even though the HITECH Act required a rule to be released by February 2012. According to reginfo.gov, the release date for this ANPRM is the same as the accounting one—November 2018.

In the absence of this regulation, OCR has kept all of its penalties. For example, in 2016, OCR collected $2.2 million from New York-Presbyterian Hospital over the "unauthorized" filming of a reality TV series that showed the death of a man in an emergency room; neither he nor his family members who were in a waiting room were aware they were being recorded and had not given consent. Although the man's image was scrambled, his widow later recognized him and family

PATIENT PRIVACY COURT CASE

This monthly column is written by Jenny Harrison of Morgan, Lewis & Bockius LLP in San Francisco. It is designed to provide RPP *readers with a sampling of the types of patient privacy cases that courts are now hearing. It is not intended to be a comprehensive monthly survey of all patient privacy court actions. Contact Jenny at jenny.harrison@morganlewis.com.*

◆ **California Supreme Court allows the Medical Board of California to access patient records.** On July 17, 2017, the California Supreme Court held that the Medical Board of California did not violate patients' right to privacy under the California Constitution when it obtained patient information from California's prescription drug monitoring program. In November 2008, the board initiated an investigation into Dr. Alwin Carl Lewis for allegedly over-prescribing drugs. During this investigation but without a warrant or subpoena, the board obtained data regarding Lewis' patients from California's Controlled Substance Utilization Review and Evaluation System (CURES). The board filed an accusation against Lewis and an administrative law judge concluded that he engaged in unprofessional conduct, engaged in negligent acts, and failed to maintain adequate records. Lewis sought to set aside the decision, arguing the board violated fundamental privacy protections in obtaining his patients' data. The California Supreme Court upheld the board's disciplinary decision, holding that the acquisition of the patient data without their authorization was justified due to the public health and safety concerns regarding regulated drugs and therefore any invasion of privacy was outweighed and justified. *(Lewis v. Superior Court of Los Angeles County, S219811; Opinion Filed 7/17/17.)*

members sued the hospital and filed a complaint to OCR *(RPP 5/16, p. 1)*.

OCR may need significant time for the process of issuing both ANPRMs. The Trump administration has required that agencies identify two existing regulations to be withdrawn for each new one they propose.

As McGraw explained, that is part of a government-wide "effort to look at all regulations and determine whether there are provisions that ought to be modified or eliminated in circumstances where they impose burdens that are out of synch with the benefits that they generate."

Contact Herold at rebeccaherold@rebeccaherold.com and McGraw at deven.mcgraw@hhs.gov. For an archive of their webinar session, visit http://tinyurl.com/ybzyehhh.✧

Revised 'Wall of Shame' Reveals Investigations, Details of Closures

The Office for Civil Rights (OCR)'s revised "Wall of Shame" website is garnering mixed reviews from industry stakeholders, who say the search functions are generally easier to use but that the tool's developers included some confusing elements while leaving out information consumers could find useful.

The new HIPAA Breach Reporting Tool (HBRT) website, which debuted July 25, is designed to focus more closely on recent breaches of protected health information. That's why it places all breaches older than two years—including those with still-open investigations—into an "Archive" section. It also includes what OCR describes as "improved navigation to additional breach information."

Still, "it's not likely that a privacy professional will appreciate any differences, other than having fewer closed issues to sort through," says Regina Verde, corporate compliance and privacy officer for the University of Virginia Health System.

"The former site was not difficult to navigate. However, it did begin to groan under the weight of the numerous breach entries. Segregating the entries on the basis of age ideally should result in a more focused and efficient search process, if one keeps in mind that the Archive label is linked only to the age of the report, not active or open case status. All told, I would not categorize the updated site as 'easier to navigate,'" Verde tells *RPP*.

Sumaya Noush, a Chicago-based attorney in the health care practice at Drinker Biddle & Reath, LLP, says the newly improved HBRT provides the same information its predecessor did—with a few new features and easier search functionality."

Noush tells *RPP* that "this new tool makes it easier—and faster—to find the information you are looking for," and that the new HBRT is "nudging the industry" towards greater awareness and accountability for health care cybersecurity, as envisioned in the Health Care Industry Cybersecurity Task Force report released June 2 *(RPP 7/17, p. 7)*.

"We expect health care industry participants to use the tool not only to flag which of their competitors/vendors/partners need to improve HIPAA compliance, but to also view the range of common vulnerabilities and breaches and follow-up with specific assessments and appropriate security measures for their own organizations," Noush says, adding, "we expect health care industry participants to learn from each other's HIPAA-related growing pains."

OCR implemented the changes following feedback over time from the public and industry—not specifically in response to the cybersecurity task force's report. "The information on the HBRT is the same information as was available on the website previously—it is just better organized," a spokesperson tells *RPP*.

However, for the first time, OCR has highlighted which cases it is investigating. The OCR spokesperson also called attention to details included in the archive section.

"There is tremendous opportunity in being able to share information with industry in a more user-friendly manner that better highlights the recent breaches, as well as the types of breaches that are occurring, industry-wide or within particular sectors, and communicates more effectively how these breaches are commonly resolved following investigations launched by OCR. The improved navigation and features provide consumers with greater access to timely information and ease of use," the spokesperson says.

Closed Cases, Older Open Cases Now Archived

The most obvious change, according to Verde, is the archive tab that contains information on older breaches. "This can be helpful as this database contains numerous line items—perhaps more than any regulator initially envisioned—and allows the user to narrow their search," she says.

In addition to moving cases older than two years to the archive, the HHS spokesperson says that breaches less than 24 months old that have been resolved have also been moved into the archive.

Verde notes that the "Research Report" link in the archive section contains the lists from both the "Under Investigation" and the archive sections. "So this is a link one could use to search the entire database," she says, but adds, "but why is it only available under the archive section?"

It seems odd, Verde says, that active cases appear in the archive section, simply because they are older than 24 months. "As an industry stakeholder, if I need to research a case, I should have enough data elements to search efficiently as all the columns are sortable, and there is an 'advanced options' search support function," she says.

Recent Trends Easier To Spot

The delineation between newer and older breaches means that "recent HIPAA breaches receive a higher level of public shaming," Noush says. "Industry stakeholders can look to this current list of investigations to determine who breached, why they breached, and whether there are any new trends of which they should be aware."

Noush points out that "some recent breaches reflect old problems, such as leaving laptops unattended in parking lots. Others result from more sophisticated intrusions, like email phishing or network hacking." In addition, she says she likes the feature that provides descriptions for many of the breaches with "a quick narrative overview of the incidents leading up to the breach."

Although a major goal voiced by OCR was to provide more help for consumers, Verde says she finds the new "Help for Consumers" tab to be somewhat confusing, in part due to what it omits. "We should expect that consumers with general questions or concerns that won't fall into a 'Wall of Shame' category may be surfing this site as well, and this section only guides the consumer to a thought process and resources regarding identity theft, suggesting they request a copy of their records and/or request an amendment to their health information and supplying a link to the FTC [Federal Trade Commission] website," she says.

The HBRT could be an ideal location to provide more general information on patient privacy rights, such as guidance on how to contact officials to report concerns, but the site doesn't do that, Verde says. "I find that web page to be lacking in providing broader resources to consumers."

HHS said in its announcement that it intends to expand and improve the site over time to add functionality and features based on feedback it receives, and the HHS spokesperson notes that the feedback the agency has received on the changes has been positive.

View the new HBRT at http://bit.ly/1FrWfKp. Contact Verde at RV5H@hscmail.mcc.virginia.edu and Noush at sumaya.noush@dbr.com.✧

With HIPAA in Check, E-Consults Expected to See Greater Adoption

Telehealth most often brings to mind providers "seeing" patients in areas with scarce medical care or for remote monitoring of symptoms. But an emerging form of telehealth that facilitates electronic referrals and consultations between primary care physicians (PCPs) and specialists is attracting acclaim, and supporters are certain it will catch on.

"Good things happen when doctors talk to each other—on a secure platform," says Paul Giboney, MD, who, in his words, runs the world's largest implementation of an e-consult program "in an open system."

Today, adoption of e-consults, as they are broadly known, is at less than 5% among health care providers and plans, says Giboney, director of specialty care for the Los Angeles County Department of Health Services, which began deploying an e-consult program with a vendor called Safety Net Connect in 2012. Its program has now grown to 18,000 consults per month involving 4,500 PCPs and 550 specialists in more than 60 specialties.

Communications Become More Secure

As far as adoption nationwide, "the sky's the limit," Giboney tells *RPP*. "People are realizing we need to do a better job in medicine of coordinating care, in integrating primary and specialty care doctors [and] making sure they are connected well. I think it's a great way of leveraging scarce specialty resources. We are so much more effective in our use of specialists now. We're not wasting visits. It's incredibly patient-centric. Patients aren't taking unneeded days off of work to go to specialty visits that could have been managed electronically with a conversation between their primary care physician and their specialist."

And, there are side benefits as far as HIPAA goes. Formal e-consult programs impose constraints and security on the electronic chatting that goes on today, often with little regard for security. Without the protections that an e-consult program can provide, covered entities (CEs) and business associates (BAs) that engage in unsecure communications face significant risk of data breaches and enforcement action, both from the HHS Office for Civil Rights (OCR) and state attorneys general as well as insurance commissioners.

To date, e-consult and e-referral are basic terms that aren't copyrighted or trademarked and are spelled in various ways and with differing capitalizations. A range of services may be offered. Programs may, for example, simply be a way to request a referral with a specialist (an e-referral), or they may permit a conversation with a specialist who can give advice for further tests and perhaps develop a treatment plan for the PCP to carry out (an

e-consult). Specialists performing e-consults can also tell the PCP when a patient needs to be seen by a specialist, which may be that individual or a colleague.

"This is not email. This is not texting," Giboney adds. "This kind of communication needs to be done [on] a medical grade, highly secure platform that hopefully has the same kind of features as your electronic health record does."

Nowadays, "there's a lot of emailing going on between doctors, a lot of stuff being sent back and forth on phones," he says. "That's not the way this should be done."

L.A. County partnered with L.A Care Health Plan, "our local Medicaid health care plan," and in 2011, started rolling out the e-consult program. The Safety Net Connect system uses a website to bring together physicians at 190 different locations "using probably 30 to 40 different electronic health records" to submit requests for consults and referrals. Safety Net Connect is a BA of L.A. County.

Office Staff Have Limited Access

Any physician who is in the network and wants help from the county's specialists is required to go through e-consult. The county doesn't pay its specialists extra to provide information through e-consult, but considers it part of their duties.

The e-consult website can also interface with L.A. County's EHR for patients who have a medical record number, and it will populate the EHR with a completed e-consult.

The website also has a number of security and operational features that help ensure the PHI is safeguarded. Users are not able to download any information or images from the website, although uploading is allowed. Physicians are the only users who can actually follow through on a request or a consult—a process that may thwart inappropriate sharing of credentials that sometimes occur in busy practices.

"We've made it crystal clear to people that sharing a password is in no manner acceptable. We need to know who's on [e-consult], and if they share their password and we find out, their access to the system will be terminated and they could lose their job. We do allow their authorized staff members also [to] access to the system but they can't submit" a request for a consult, he says. "Let's say they have a referral coordinator or a nurse that is helping them in the care of their patient in the clinic. That nurse or that referral coordinator can cue up the consult for them. They can select the specialty, associate it with the right patient, attach the relevant medical information, then they do what's called 'saving it as a draft' within e-consult. Then an alert goes to the PCP and says, 'Hey you've got a draft waiting for you,'…they go on to the system, sign on, get the draft, review it for accuracy. They are the only ones that can pose the clinical question to the specialist and they are the only ones that can click 'submit.'"

While security concerns exist, they aren't overwhelming and they can be addressed.

"Any time patient data is in the electronic information it's vulnerable. But, so are charts," says Giboney. "People could grab a chart and walk out the door. Security concerns are just different now because of the electronic storage."

De-identified Information Can Also Be Shared

Three-year-old RubiconMD sells a different form of e-consult. The Irvine-based firm offers consultative services in 32 states, says J. Nwando Olayiwola, M.D., an associate professor in the Department of Family and Community Medicine at the University of California, San Francisco. Olayiwola was named RubiconMD's first chief clinical transformation officer in January.

RubiconMD "stores the information…in a HIPAA-compliant way," she says, and "enables that communication to happen in as close as possible to real time." Rubicon has a stable of specialists across the country, which allows a PCP "to get access to a specialty opinion within 12 business hours."

Often the response is even sooner—within four hours, according to Olayiwola.

One safeguard is that the information exchanged "is blinded. All the PHI is redacted before the specialist gets the actual consultative request," Olayiwola explains. Even so, RubiconMD considers itself a BA and complies with HIPAA.

Like Giboney at L.A .County, Olayiwola also expects e-consults to see expanded acceptance, especially as primary care practices seek to become more patient-centered.

"I think over the next few years we will see a tremendous amount of growth," Olayiwola says. Currently "it's the smaller practices that are engaged…but many of the large systems are also moving towards this."

In fact, by the end of this year, the San Mateo County Health System plans to implement both e-consult and e-referral programs. The system includes San Mateo Medical Center, which consists of eight outpatient clinics and 10 affiliated clinics. The system has spent years planning for implementation and will be using AristaMD, Inc., as its vendor.

"An eConsult is when a primary care provider asks a specialist for assistance in the treatment of a patient. The response may be as simple as confirmation of a treatment plan. The new program will facilitate that function, making the data part of the patient's record," Shawn Savadkohi, the health system's information

security officer, tells *RPP.* "An eReferral is when a primary care provider requests a visit with a specialist. The program will ensure that all diagnostic testing outlined by our specialists will be completed prior to scheduling a referral visit to ensure a successful specialist visit. In addition, the program will communicate the outcome of this visit with the referring provider."

San Mateo is "in the execution phase of the project," with the vendor planning to make a presentation to a steering committee early this month, Savadkohi says. Ultimately, 500 physicians, 300 nurses and 125 physician assistants will have access to the program. A 60- to 90-day pilot will involve primary care physicians and specialists in rheumatology and musculoskeletal care.

At least initially, San Mateo providers will "work both in their EMR [electronic medical record] and the eConsult portal. To avoid redundant data entry and errors, auto population of data is performed where possible. Because specialists are part of the San Mateo County Health System, sharing is not necessary as they already have access to the required patient information," Mike Aratow, M.D., San Mateo's chief medical information officer, tell *RPP.*

"Security of ePHI is constantly a concern," Savadkohi says. "San Mateo County Health System has a process to review all prospective contracts and scope of work for acceptable security controls prior to signing. This risk management practice helps us identify security gaps that we can negotiate with the vendor ahead of time. These can then be corrected as part of contract revisions, and monitored for inclusion when the technology is implemented. In the case of eConsult, a risk management assessment was completed with the vendor during contract negotiations. It is included with the review documentation."

Tips for Implementation

RPP asked the proponents of e-consult programs for suggestions on how to make implementation successful. One key has been the assistance of grant funds, as neither Medi-Cal nor private insurance firms cover e-consults yet.

Last year RubiconMD received a boost when the California Health Care Foundation made a $750,000 "investment" in the firm "to "improve access to health care for consumers in low-income or underserved communities in California."

In addition, the Blue Shield Foundation of California has helped fund e-consult programs. It has provided more than $1.5 million for "multiple local" e-consult programs, including to L.A. County's.

According to the foundation, "there are two important lessons learned to date: 1) You must have a clear understanding of your system's specialty access needs and gaps in care; 2) Bring together primary and specialist physicians early and often—their engagement and willingness to collaborate is vitally important."

The foundation also called attention to "a growing repository of best practices and information to facilitate the process and help ensure its success. Building from expert input, case studies, evaluation and research, [it] developed the resources below to help guide the implementation of eConsult systems in communities across the state." These can be found here: http://tinyurl.com/ybrehjzl.

"Having a solid risk management plan paired with established security standards defined in your organization is a key to success," says San Mateo's Savadkohi. "Be prepared to have the means and methods to assess security at different lifecycle phases. Conduct security control reviews prior to contract, at implementation, and during change actions to ensure those controls remain effective."

Contact Giboney at pgiboney@dhs.lacounty.gov and Olayiwola at nwando@rubiconmd.com. For information about San Mateo's program, contact Diana Rohini LaVigne at dlavigne@smcgov.org.✧

Beware of HIPAA When Responding To Negative Reviews Posted Online

As medical review sites proliferate and cumulatively rack up millions of views per day, physicians and health care systems need to understand what they can—and often more importantly, can't—say online in response to a negative review.

Consumers who frequent online review sites for other industries are accustomed to seeing responses to reviews, especially to negative reviews. But "hands are tied for the provider," says health care law attorney Robert Coffield, who practices with Flaherty Sensabaugh Bonasso PLLC in Charleston, W.Va. "The [HIPAA] rules don't allow them to actively participate in the discussion," Coffield tells *RPP*.

Health care providers—or their representatives—can engage people online who post negative reviews, but they need to be extremely cautious when doing so, other medical privacy experts also say.

"When patients are looking at reviews, they want to see a response back," but health care practitioners must be mindful of HIPAA privacy rules at all times, says Andrew Rainey, executive vice president of strategy and corporate development for Binary Fountain, which provides patient feedback management solutions designed specifically for health care.

Rainey tells *RPP* that he recommends responding briefly online, but then shifting the conversation out of the public space to a secure platform as quickly as possible.

"It obviously makes sense to respond to negative reviews," says Rainey. "But that's not to say it makes sense to respond to all of them. You get a feel for what type warrant a response. I understand frustration on the physicians' side, but consumerism is very real."

When HIPAA was enacted and the regulations were written, social media didn't exist, Coffield says. Therefore, stakeholders are attempting to apply it in a way that wasn't envisioned at the time, he says, adding, "I think a lot of people have struggled with it."

Over the past seven or eight years, Coffield says, physician and hospital clients evolved on their thinking about implementing a social media policy. Initially, he says, most organizations avoided all social media, due to HIPAA regulations. But as social media has matured, "it starts to get to the point where we have to let [employees] on social media to do their job."

"My sense and my recommendation is, you want to work towards a pro-social media policy that educates and informs employees what they can and can't do on social media" to comply with HIPAA, Coffield says. "You almost can't sit back and not respond" to negative feedback, since failing to respond looks far worse than a HIPAA-compliant response. "You need to have a well thought-out policy to respond."

Medical Rating Sites Abound

Reviews come in a variety of formats on a growing number of websites, and can range from simple star ratings to anonymous essays. Different sites handle comments and reviews in varying ways:

◆ Facebook offers an option for businesses to add a space for reviews to their pages, but clients also can leave public comments on a business or personal timeline. Either way, the physician or health care entity in question can post a response or open a dialogue. Most people on Facebook post under their own names.

◆ Twitter doesn't offer a reviews option—instead, users can post and share comments, called tweets, that "tag," or identify, a subject such as a physician or hospital. The physician or hospital in question can respond by replying to the comment. Twitter is not primarily a review site, and it does not gather reviews in one place. Some people use pseudonyms on Twitter.

◆ Yelp, which is better known as a site to find restaurant and hotel ratings, also has a plethora of reviews for doctors, hospitals and other health care facilities. Entities can post responses to reviews, and many do so. Yelp users can post under their own names, but most do not.

◆ Zocdoc combines reviews and appointment scheduling, offering users the ability to search physicians and other health care providers by specialty and insurance accepted, and then schedule an appointment via the app or website. Reviews can include first names, and Zocdoc notes when a reviewer is a "verified patient."

◆ RateMDs, a site specifically for doctor reviews and ratings, allows anonymous written reviews and provides health care practitioners with the opportunity to write a response to those reviews. The site has more than two million ratings.

◆ Healthgrades, which has high web traffic, has come in for plenty of criticism from health care practitioners because it allows anonymous reviews without verification that the reviewer is a patient. The site does allow providers to respond to negative reviews, but physicians have cited HIPAA concerns as part of what they say is an inability to properly refute unfair reviews.

Some sites, such as WebMD, allow users the chance to provide a star rating for a health care practitioner or facility, but don't give the opportunity for comments from the reviewers or responses from the practitioners.

Offer To Speak with Unhappy Patients

Physicians and other health care entities cannot respond directly to specific patient complaints in negative reviews, Coffield says.

"You can either be silent, or if it's your patient, you can follow up directly with the patient," he says, adding that it's best to bring the patient into the office to deal with the complaint directly, person-to-person. "You can't respond [like that] online," or even by phone, he emphasizes, even though he acknowledges that "it's difficult for physicians to do, especially older physicians where they're used to compliant patients."

Replying directly online, even without addressing specific complaints, has to be done extremely carefully in order to comply with HIPAA regulations, Coffield says. He adds that a HIPAA-compliant response might read something like: "This website is not the proper forum for these types of discussions. If you have an issue with this particular provider, contact the facility."

He adds, "You should respond in almost a webmaster-type fashion, and then immediately call the person [if the person can be identified] and say, 'I just saw your post, and I'd like you to come in and talk about it.'"

There shouldn't be anything problematic about responding to a negative review by saying, "Please give me a call at this number," Coffield says. But getting into detailed discussions—even through Facebook and Twitter's private messaging systems—is "pushing the envelope."

"A lot of providers think if they don't say who the patient is or don't divulge many details that they're not violating HIPAA—they're keeping confidential information confidential," Coffield says. However, protected

health information under HIPAA includes information that could give someone the ability to identify a patient, and social media posts that include even scant detail could do that, he says.

Anonymous reviews pose even more significant problems, Coffield says. "Engaging validates the patient on the other side, and with some of these people you can't win—the more you engage, the more you anger them. But at the same time, failure to respond at all might anger them, even if the response is, I'm not going to respond." In those cases, provider organizations should attempt to take the discussion offline, but also should be prepared to stop engaging entirely, he says.

Develop a Response Policy for Reviews

Binary Fountain works with clients to manage their social media presence. When it comes to review sites, Rainey says, most feedback tends to be positive or neutral, but it appears more realistic for the provider to have a few less-than-stellar reviews in the mix: "You want to have a mix of positive and negative reviews."

Deciding to respond online to negative reviews, even in a minimal, HIPAA-compliant fashion, requires a case-by-case analysis, says Rainey. For example, if a provider only has two reviews, and one is negative, then "maybe" it would be worth a response to balance out the negativity, he says, although "obviously not with any level of detail" that speaks specifically to outcomes or to anything identifiable about the case.

On Facebook, where names are clearly visible and usually real, Rainey suggests replying to negative comments using language like this: "I'm sorry to hear about your negative experience. We strive to ensure that these negative experiences don't happen to anyone." Then the reply should urge the person to call or email the office, in an effort to "take the conversation offline."

For example, Binary Fountain client Providence Health & Services, based in Renton, Wash., responded to a negative Facebook post from a man who said he was disappointed in his care: "This is certainly not the feedback we like hearing from our patients, Dave. We strive to provide each and every one of our patients with the highest level of compassionate care possible. Thank you for taking the time to share about your experience, as it is what helps us to improve our overall quality of service."

Other hospitals take a similar approach. For example, Sentara Regional Medical Center in Williamsburg, Va., responded to a negative review by saying: "We always strive to give the best patient care and are very sorry to see this happened to you and your wife. Please send your contact information to 1800Sentara@Sentara.com so we can route you to the appropriate patient advocate and learn more."

On Yelp, the approach is again similar, even if the reviews are anonymous. Northwestern Memorial Hospital in Chicago responded to a recent negative review by saying: "Thank you for your honest feedback and we are sorry to hear about the troubles that you've experienced. If you haven't already spoken with our Patient Relations Department, please fill out the following online form and our team will be in touch to help. Thank you."

Twitter requires shorter replies—it's limited to 140 characters—but the format still allows for the standard "please get in touch" approach recommended by experts. For example, an anonymous Twitter user tweeted at Providence Health & Services recently, saying "@Prov_Health thanks for costing me thousands of dollars. Worthless criminals should [be] ashamed." Providence replied, "Is there something we can help you with? Please dm [direct message] us and we are happy to look into your concern."

Doctors Advised to Remain Mum

It's important to train physicians not to respond directly and impulsively to negative reviews, Rainey says.

"We see physicians who do take this very personally," he says, adding that "we do not recommend the physician respond back—oftentimes that's going to involve 'shooting from the hip.'" Responding to negative online reviews or comments in an emotional manner can result in major HIPAA problems, he adds.

"Inherently, it is incredibly challenging for the average patient to provide an accurate review of the quality of care they received," Rainey says. "And it's not just the quality of the procedure—it's the parking, the quality of the front desk staff," and other factors, some of which are not under the provider's control.

Instead of the physician responding directly to negative comments, an established marketing team—assuming one is in place—can be trained and tasked with formulating responses, he says. The message from that marketing team to physicians should be: "Please do not go and create your own account and respond to this."

Appropriate, measured responses can sometimes even persuade a reviewer to change the review, Rainey says. In one case, he says, a reviewer posted a negative review of a large hospital system's emergency department on Yelp, but revised the star rating upward after the emergency room director reached out personally.

Contact Coffield at RCoffield@FlahertyLegal.com and Rainey via Binary Fountain spokesperson Michiko Morales at michim@gabrielmarketing.com.✧

'Hardening' Workforce Reduces Risk

continued from p. 1

Touhill tells *RPP* his approach toward HIPAA compliance stresses ensuring a proper balance between investments in technology and in the workforce. "If you gave me an extra dollar in cybersecurity I was going to spend it on people," Touhill says. People, he points out, "are your greatest resource but they're also your weakest link."

Based on feedback from "incident response teams" that reported to Touhill and what he personally saw, he says that "organizations that had really good balance minimized their risk. And those that relied solely on technology and really didn't invest well in their people were the ones who had the greatest risk [of negative impacts] due to incidents. I believe you can buy down your risk by investing well and balancing between technology and people."

The NIST framework is central to both IT and non-IT compliance efforts, in his view. Released in 2013, the framework is now being updated as a result of a report by a federal cybersecurity task force *(RPP 7/17, p. 7).* On May 17, 2017, President Trump issued an executive order, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," which requires all federal agencies to implement NIST's framework "to manage the agency's cybersecurity risk."

Previously, experts have also advised health care organizations to use the framework to aid in HIPAA compliance.

In 2016, the HHS Office for Civil Rights (OCR), which enforces HIPAA, issued a "crosswalk" that matches requirements in HIPAA regulations to those in the framework (for information, see http://tinyurl.com/y9yukt42).

In his experience investigating and mitigating security incidents, Touhill says these nearly always "track[ed] back to a human failure…failure to patch, failure to configure correctly, failure to read the instruction book."

Among the goals in developing a well-trained and well-prepared workforce is to "build in resiliency."

Resilient members of such a workforce, says Touhill, "know what to do. They know when to do it. They know how to do it. And when a really bad day occurs and they're confronted with the unknown, something that you didn't anticipate, that they're resil-

OCR Offers Tips on Training for Security Rule Compliance

The HHS Office for Civil Rights (OCR) tackled the issue of employee training in its July "cyber awareness" newsletter, expressing many of the same concepts that Greg Touhill, formerly the nation's chief information security officer, shared with *RPP* (see story, p. 1).

"An organization's training program should be an ongoing, evolving process and flexible enough to educate workforce members on new cybersecurity threats and how to respond to them," the newsletter says.

Regarding training, HIPAA-covered entities and business associates should assess how frequently to "train workforce members on security issues, given the risks and threats to their enterprises, and how often to send security updates to their workforce members. Many entities have determined that bi-annual training, and monthly security updates are necessary, given their risks analyses."

◆ Consider utilizing "security updates and reminders to quickly communicate new and emerging cybersecurity threats to workforce members such as new social engineering ploys (e.g., fake tech support requests and new phishing scams) and malicious software attacks including new ransomware variants."

◆ Determine the "type of training to provide to workforce members on security issues, given the risks and threats to their enterprises. Computer-based training, classroom training, monthly newsletters, posters, email alerts, and team discussions are all tools that different organizations use to fulfill their training requirements. OCR has training materials available, including Medscape training modules on security of PHI." Visit https://www.hhs.gov/hipaa/for-professionals/training/index.html and http://www.medscape.org/sites/advances/patients-rights.

◆ Remember to "document that training to workforce members was provided, including dates and types of training, training materials, and evidence of workforce participation. Any investigator or auditor will ask for documentation, as required by the HIPAA Rules, to ensure compliance with the requirements of the Rules. See 45 C.F.R. §§ 164.316(b) and 164.530(j)."

For the full July newsletter, see http://tinyurl.com/y7zrwmvm. The monthly newsletters are available online at http://tinyurl.com/ycptkn6c. They are also sent by email to subscribers.✧

ient enough to act in the proper manner that's going to minimize your risk."

This is achieved, he says, through "training, awareness, practice and repetition," without letup. As Touhill put it, attacks "are going to keep on coming in the cyber world," and so must efforts to thwart them.

Touhill offers the following suggestions as the foundation for hardening the workforce.

"First, you have to identify information as an asset in your workforce," he says. "Too many people try to defend all information equally. Clearly, you have some high value information and you probably have some information that you don't think is as high a value. You really want to know what type of information you have and protect it based upon its value."

Touhill likens this to what the military designates as its "key cyber-terrain." In addition, organizations need to identify "what doesn't necessarily need to be as protected."

Second, using the NIST framework, which focuses on "protecting, detecting, respond[ing] and recovering," Covered Entities and Business Associates should "identify the tools, technology and people requirements to adequately meet the needs of that risk framework."

Third, "train your people relentlessly to execute" the plans for threat detection, mitigation and recovery. As Touhill notes, "Training is more than just a 'one-and-done.' You need to continually exercise your skills" through drills. Training also needs to be freshened and updated with the newest threats of the day.

Strive for 'Perfect Practice'

Training to guard against phishing can also be focused on the "READ" framework, which prompts workers to take the time to spot fake and potentially malicious emails, he explains. The R means read the email and see if it is relevant; E refers to whether the email was expected; A is a trigger to see if the email is authenticated; and D is for a digital signature, which may be present and can confirm that the email isn't fraudulent.

Remind workers that, "'when in doubt, pick up the phone to call the person' who seems to have sent the email, before clicking on a suspicious link or downloading a document," Touhill says.

For cybersecurity, the admonition of "practice makes perfect" isn't enough. Better is "perfect practice makes perfect," as intoned by Vince Lombardi, says Touhill. "Organizations that practice can buy down their risk against spear phishing, ransomware attacks, and the like," he says.

"We had a program at an organization that I used to lead where every quarter we would send out phishing messages [purportedly] from our top boss," which misspelled his last name.

He recalls that the first time this was tried, some 200 people out of 1,200 fell for the ruse. With repeated exercises, the number was to just eight, Touhill says.

Workers who made the mistake "had to come see the big boss," says Touhill. "They didn't get in trouble to the point where they got fired." But the personal visit "heightened their awareness and because there was leadership involvement it certainly helped buy down our risk."

The exercise Touhill described is similar to efforts undertaken by United Health Services (UHS) of Birmingham, N.Y., several years ago *(RPP 3/13, p. 1).* At the time, such activities were rare, UHS officials said. UHS emailed workers a link that sent them to the systems intranet and it asked for credentials. Once those were entered, a virus was activated that grabbed workers' credentials and permitted access to UHS systems.

Foster Education Through Sanctions

Asked how CEs and BAs should structure their sanctions programs, Touhill responds that he has "seen very successful organizations that take things on a case-by-case basis but, frankly, nearly every single one has 'a three strikes and you're out'" approach.

Regardless of what they are, sanctions should be "clearly articulated" to the workforce by its leadership, says Touhill.

"With that said, good people do make mistakes at times and having that clearly spelled out that, 'Hey, if you do misuse this deliberately you could be fired and you probably will,' that's a pretty good attention-getter," he says. "However, you have to have a very good and well-defined handbook there for the managers for the folks that do minor things. You don't want to take away the ability of managers to train as well as continue to educate."

Adds Touhill, "you don't want to lead by fear; you want to lead by example."

Of course, workers need to have updated technology to assist them. Leaders need to pay attention to the age of devices and other equipment, he says. Once the device is too old to be patched, "it's time to recapitalize. You need to retire some of your old stuff if you are going to be connected to the internet."

"We need to be very discriminating customers in the health care world," he adds, and demand better security, especially from devices and products that connect to the internet. "A lot of the operational technology is still not secure. It was just built to work and not necessarily with security included in that [as a] baseline requirement."

Contact Touhill at cyxtera@teneostrategy.com.✧

PRIVACY BRIEFS

◆ **A ransomware attack at an obstetrics-gynecology clinic in Oaks, Pa., may have compromised data for 300,000 patients.** The Women's Health Care Group of PA posted a notice on its website on July 18 that a server and workstation at one of its practice locations had been infected by a ransomware virus. "As part of our investigation, we learned that external hackers gained access to our systems, as far back as January 2017, through a security vulnerability. We also believe the virus was propagated through this vulnerability," the clinic said in its statement. Files that may have been accessed include Social Security numbers and medical information. The clinic said the FBI has been notified. Read the full notice at http://bit.ly/2tJHVhC.

◆ **Anthem, Inc., which in June okayed a $115 million settlement in a class action data breach lawsuit (*RPP* 7/17, p. 1), suffered another privacy-related setback** when a data breach by a contractor may have exposed personal health information of more than 18,500 Anthem Medicare enrollees. Anthem says that consulting firm LaunchPoint Ventures contacted it about the breach on June 14. LaunchPoint told Anthem that an employee stole Anthem members' Social Security numbers and Medicare identification data, mailing the data in a file to his personal email address more than a year ago. Read more at http://cnb.cx/2vZV9Ec.

◆ **Peachtree Neurological Clinic in Atlanta discovered a breach in its computer system while investigating a ransomware attack that turned out to be unrelated.** According to the clinic's statement, its electronic medical records were encrypted by the ransomware. Peachtree didn't pay the ransom; instead, it used backups to restore its files. But in the process of investigating the ransomware attack, it found that its computer system had been accessed by unauthorized individuals between February 2016 and May 2017. The clinic couldn't tell what exactly was accessed, but said it's possible that the electronic medical record system was breached, which would have exposed personal and medical information. View the clinic's statement on the breach at http://bit.ly/2vsVIsW.

◆ **Nearly half of health care organizations use both in-house and contracted services to manage their cybersecurity, a Medical Group Management Association Stat poll shows.** The poll found that 31% of organizations manage their security entirely in-house, while 21% outsource it completely. Many health care organizations said they outsourced part of their security needs because their in-house staff didn't have the capacity to handle everything. Get more information and see the poll's results at http://bit.ly/2vCZIYf.

◆ **U.S. consumers are far more worried about theft of Social Security numbers and banking information than they are about theft of their medical records and biometric data**, according to a survey from credit reporting firm FICO. Some 86% said they had concerns about their Social Security numbers being stolen, while just 15% said they worried about their medical records. View all the findings at http://bit.ly/2vsK01h.

◆ **A Roanoke, Va.-based accountant with no links to health care entities says he's been receiving faxes with protected health information for four years**, and he hasn't been able to stop them, even though he has spent hours trying to do so. The accountant says he's received at least 100 faxes, most with names plus detailed medical and diagnostic information. He says he suspects his fax number mistakenly is listed in local directories of health care providers. View the story at http://bit.ly/2ucqRwy.

◆ **U.S. Sen. Richard Blumenthal (D-Conn.) has introduced legislation to protect patients' medical information from hackers by requiring cybersecurity protections for medical devices**. The bill, unveiled Aug. 1, would create a cyber report card for devices and mandate testing prior to sale. It also would bolster remote access protections for medical devices, and ensure crucial cybersecurity fixes or updates remain free and not require Food and Drug Administration recertification. See the announcement at http://bit.ly/2fi5Xd6.

◆ **The University of Vermont Medical Center reports that 2,300 patients' medical information may have been compromised in May** when an unauthorized third party gained access to an employee's email account. Social Security numbers and financial information were not included in the potential breach. Read the notice at http://bit.ly/2v9BkdF.

◆ **Plastic Surgery Associates of South Dakota says a ransomware attack may have exposed some patient records to hackers.** The company says it is notifying about 10,200 people that their records may have been affected, although investigators say it's likely few patient records were accessed. The information impacted could include Social Security numbers and medical information. Learn more at http://argusne.ws/2ve0ISt.