SEPTEMBER 2021 | VOLUME 21 | NUMBER 9

tci Newsletters

Health Information Compliance Alert

Timely News & Analysis On HIPAA, E-Health, Privacy, Security & Technology

We welcome your comments & suggestions!

E-mail **Kristin J. Webb-Hollering**
Development Editor, at:
kristin.hollering1@aapc.com

To subscribe or request help with your current subscription, call: 1-800-874-9180 or e-mail: service@codinginstitute.com.

Case Study

Follow Through With Security Rule Requirements

Tip: Feds want to see that you've addressed your risks with a compliance plan.

If your practice is doing an annual security risk analysis, that's great. But, if you find yourself on the wrong side of a breach, you'll need more than an analysis of your risks to convince the HHS Office for Civil Rights (OCR) that you're serious about HIPAA compliance.

Background: Many providers, especially those who participate in federal healthcare programs, perform security risk analyses to comply with Promoting Interoperability requirements, but HIPAA compliance with the Security Rule requires much more than just assessing the risks. After evaluating the potential problems, covered entities (CEs) are tasked with "implement[ing] appropriate security measures to address the risks identified in the risk analysis; document[ing] the chosen security measures and, where required, the rationale for adopting those measures; and maintain[ing] continuous, reasonable, and appropriate security protections," reminds the OCR summary of the Security Rule.

Last January, the feds amended the HITECH Act, requiring the HHS Secretary to consider specific "recognized security practices" when investigating HIPAA violations. If CEs and their business associates (BAs) show they've implemented the "recognized security practices" for 12 months, then OCR must consider that when deciding their audit timeline, penalties, and resolutions, suggests the amendment.

Here's the Problem

Though the amendment does define "recognized security practices" as "standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act" and "the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015," it gets a little hazy after that.

This latest HITECH amendment, similar to the language of the Security Rule, allows providers a considerable amount of leeway to determine the route they want to take with designing and implementing HIPAA compliance. There are both pros and cons to this kind of flexibility, especially for providers with limited resources.

"The good news for small practices is that the government designed the Security Rule to be 'scalable and flexible,' meaning that a solo

practitioner or a two-person office does not have to implement a HIPAA compliance program with the same level of detail and investment that would be required for a large multi-state hospital system or health insurer," explains attorney **Shannon Hartsfield**, an executive partner with Holland & Knight LLP in Tallahassee, Florida. "These smaller practices have some room to maneuver when deciding exactly what they will do to comply with HIPAA's requirements. They have to comply, but they may not be required to have a compliance program that is as detailed and involved as a larger practice," she adds.

Caveat: However, size and scope don't necessarily factor into enforcement, and recent settlements have shown that OCR can be tough on smaller healthcare providers, depending on the situation.

"Small organizations can be penalized for violations. The costs of responding to a data breach add up based, in large part, on how many patients are involved, rather than the size of the entity experiencing the breach," warns Hartsfield.

Consider These Tips

Luckily, there are several things that small practices can do to build their HIPAA compliance plans — and ensure they are implemented according to the Rules. For instance, as part of its training resources, OCR offers "a beginner's overview of what the HIPAA Rules require, security training games, risk assessment tools, and other aids," online guidance says. The agency partners with the HHS Office of the National Coordinator for Health Information Technology (ONC) to provide CEs and BAs with these resources.

Even with the plethora of federal resources and guidance available, compliance planning can be daunting and complicated. "Security Rule compliance still requires significant effort and IT-related expertise so, no matter the entity's size, it may be necessary to hire qualified consultants to help with the risk analysis process," Hartsfield says. And "beyond the risk analysis, covered entities and business associates must also develop a written plan to manage and mitigate the risks identified. They must also update the risk analysis as needed," she advises.

In smaller practices, the appointed security officer needs to cultivate compliance and educate the new employees on the HIPAA Rules. Workforce compliance training needs to be ongoing and take into account both state privacy laws and federal updates, too. "Training isn't something that is given once to a new employee and never again. Training also has to be documented," says Hartsfield.

Overall, HIPAA training programs must resonate with staff, boost security awareness, and align with the CE's specific needs, policies, and protocols.

"If your workforce members have not been trained in your policies and procedures, it not only increases the risk of a data breach, but it could result in increased penalties if that breach happens," Hartsfield cautions. "Staff must be trained in the privacy and security policies and procedures they need to know in order to do their jobs and keep the data they handle private and secure."

BAs also need to up their game on HIPAA compliance, too. "Some business associates only offer employees canned training

Health Information Compliance Alert (USPS 022-061) (ISSN 1548-985X) is published monthly 12 times per year by The Coding Institute LLC, 2222 Sedwick Road, Durham, NC 27713 ©2021 The Coding Institute. All rights reserved. Subscription price is $299. Periodicals postage is paid at Durham, NC 27705 and additional entry offices.

POSTMASTER: Send address changes to *Health Information Compliance Alert*, 4449 Easton Way, 2nd Floor, Columbus, OH, 43219.

modules designed for providers, so there is a risk that the employees won't understand the special requirements for business associates. A telehealth physician may need different training than an in-person receptionist," for example, Hartsfield points out.

Resources: Check out OCR and ONC's online tools at www.healthit.gov/topic/privacy-security-and-hipaa/health-it-privacy-and-security-resources-providers. Review the HITECH amendment at www.congress.gov/116/bills/hr7898/BILLS-116hr7898eh.pdf. TCI

▶ Covid-19 Vaccinations

Know These Facts on the Intersection of HIPAA and Vaccinations

Plus: Feds, some states require COVID vaccinations for healthcare workers.

With some states requiring COVID-19 vaccinations for healthcare workers, you may be wondering how HIPAA compliance fits into the scenario. Read on for the details.

Consider These Vaccination Mandate Logistics

Rollback: In May, the Equal Employment Opportunity Commission (EEOC) expanded its guidance on COVID vaccination mandates in the workplace. "The federal EEO laws do not prevent an employer from requiring all employees physically entering the workplace to be vaccinated for COVID-19," but organizations must offer accommodations to staff that align with provisions outlined in Title VII of the Civil Rights Act and the Americans with Disabilities Act (ADA), according to May 28 EEOC guidance. Accommodations mentioned by the EEOC include face masks, social distancing, remote work, split shifts, COVID-19 testing, or if need be, reassignment to another position.

At press time, 22 states had some sort of vaccination mandate for specific healthcare workers in their states, according to the National Academy for State Health Policy (NASHP) online resources. But, the stringency of the requirement depends on the state, and policies vary significantly, carrying legal implications on both sides of the debate.

For instance, Washington state has one of the strictest mandates in the country. On Aug. 9, Gov. **Jay Inslee** issued an emergency proclamation that all state workers, volunteers, on-site contractors, public and private healthcare workers, and long-term care workers be vaccinated by Oct. 18. Though the Washington mandate offers no weekly testing option for those refusing vaccination, the state does provide "exemptions from the vaccine requirement … for those individuals who are entitled to a disability-related reasonable accommodation or a sincerely held religious belief accommodation," a release maintains.

Bans: Some states have opted to remain neutral on vaccination requirements for healthcare workers, leaving it up to the individual organizations, while others have banned such mandates. "Several states have proposed legislation prohibiting mandatory vaccination policies," point out attorneys with international law firm Perkins Coie LLP. "Montana currently prohibits employers from discriminating against a person based on the person's vaccination status. Other states have proposed similar legislation," the Perkins Coie lawyers say in online legal analysis.

Here's the HIPAA Tie-In

"If an employer asks an employee to provide proof that they have been vaccinated, that is not a HIPAA violation, and employees may decide whether to provide that information to their employer," the Department of Health and Human Services (HHS) says in a frequently asked question on Coronavirus. However, it gets a little more complicated after that data is collected.

Once that COVID-19 vaccination info is "obtained ... the vaccination status data is considered confidential medical information and must be handled accordingly," say attorneys **Anna-Liisa Mullis** and **Christine A. Samsel** with law firm Brownstein Hyatt Farber Schreck, LLP in online legal analysis.

As a covered entity (CE) or business associate (BA), you are privy to HIPAA — and your employees' COVID-19 vaccination information is considered protected health information (PHI). That means the PHI falls under the HIPAA Rules' governance.

"Employers would be well advised to provide advanced written disclosures to employees regarding the vaccination process, the legitimate business reason for same, and how the employer (or the group health plan) will use, store, and share (if at all) vaccination data of individual employees," the Perkins Coie lawyers note.

Your organization should review state privacy laws as those can be much more stringent than HIPAA and could carry penalties for noncompliance. Remember, that the Centers for Disease Control and Prevention (CDC) and Occupational

Safety and Health Administration (OSHA) offer advice on the best way to compile and store staff medical records, including COVID-19 vaccination files (see *Health Information Compliance Alert*, Vol. 21, No. 4).

HHS, VA Require Healthcare Workers to Get the Vax

Since some staff are on the front lines caring for patients, it shouldn't be a surprise that HHS is now requiring a COVID vaccination for its 25,000+ workforce.

"Staff at the Indian Health Service (IHS) and National Institutes of Health (NIH) who serve in federally-operated health care and clinical research facilities and interact with, or have the potential to come into contact with, patients will be required to receive the COVID-19 vaccine," the agency noted in an Aug. 12 release. "This includes employees, contractors, trainees, and volunteers whose duties put them in contact or potential contact with patients at an HHS medical or clinical research facility."

Additionally, members of the U.S. Public Health Service Commissioned Corps, who often assist in disaster and crisis situations and are referred to as "emergency responders," will be required to get vaccinated as well as healthcare workers at the Department of Veterans Affairs (VA), the release said.

"Vaccines are the best tool we have to protect people from COVID-19, prevent the spread of the Delta variant, and save lives," said HHS Secretary **Xavier Becerra** in a release. "Instructing our HHS health care workforce to get vaccinated will protect our federal workers and the patients and people they serve."

Nursing homes: On Aug. 18, the Centers for Medicare & Medicaid Services (CMS) announced that it, "in collaboration with the Centers for Disease Control and Prevention (CDC), is developing an emergency regulation requiring staff vaccinations

FDA Gives Pfizer Vaccine Full Approval

This may alleviate COVID vaccination mandate stress.

If your organization is swamped with COVID-19 vaccine questions, prepare yourself. One recent update may quadruple patient — and staff — inquiries.

Why? On Aug. 23, the Food and Drug Administration (FDA) moved the Pfizer-BioNTech COVID-19 Vaccine from its emergency use authorization (EUA) status to fully approved for individuals 16 and up. The vaccine is rebranded under a new name, "Comirnaty," which may confuse consumers.

But: The Pfizer vaccine will retain its EUA status for "individuals 12 through 15 years of age and for the administration of a third dose in certain immunocompromised individuals," an FDA release said.

"While millions of people have already safely received COVID-19 vaccines, we recognize that for some, the FDA approval of a vaccine may now instill additional confidence to get vaccinated," said Acting FDA Commissioner **Janet Woodcock, MD**, in a release on the change.

Experts suggest that this may decrease vaccine hesitancy. "Full approval may be welcome news to some employers, as EUA status has reportedly been a driver of hesitancy among some 30 percent of unvaccinated employees," explain attorneys **Jennifer Nelson Carney, Christopher Page**, and **James Petrie** with law firm Bricker & Eckler LLP. "Full approval also reduces employers' legal risk in mandating vaccines," Nelson Carney, Page, and Petrie point out in online legal analysis.

The FDA, in coordination with the Centers for Disease Control and Prevention (CDC), plans to continue its extensive safety monitoring of the Comirnaty COVID-19 Vaccine, but assures the "public and medical community [they] can be confident that although we approved this vaccine expeditiously, it was fully in keeping with our existing high standards for vaccines in the U.S," indicated **Peter Marks, MD, PhD**, director of FDA's Center for Biologics Evaluation and Research, in the FDA release.

Resource: See the timeline and find more information on the Comirnaty COVID-19 Vaccine at www.fda.gov/emergency-preparedness-and-response/coronavirus-disease-2019-covid-19/comirnaty-and-pfizer-biontech-covid-19-vaccine. TCI within the nation's more than 15,000 Medicare and Medicaid-participating nursing homes," according to a CMS release.

"The data are clear that higher levels of staff vaccination are linked to fewer outbreaks among residents, many of whom are at an increased risk of infection, hospitalization, or death," CMS Administrator **Chiquita Brooks-LaSure** said in the release.

About 62 percent of nursing home staff are currently vaccinated, CMS said. (CMS requires nursing homes to report that data.) "Vaccination among staff at the state level ranges from a high of 88 percent to a low of 44 percent," the agency reported. Many recent COVID outbreaks have been "occurring in facilities located in areas of the United States with the lowest staff vaccination rates," CMS added in the release.

The agency plans to issue the vaccination requirement sometime in September.

Disclaimer: Information related to COVID-19 is changing rapidly. This information was accurate at the time of writing. Be sure to stay tuned to future issues of *Health Information Compliance Alert* for more information.

Resource: See the EEOC guidance at www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws#K.

Toolkit

Beef Up Your Cybersecurity Glossary With These 7 Definitions

Feds warn of ransomware attacks on weekends and holidays.

Whether your organization supports staff working remotely or you're revisiting virtual options to combat COVID surges, you need to be mindful of the security risks. And, now the feds advise IT staff to prepare for the heightened threat of cyber attacks during downtimes.

Details: The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) issued a joint cybersecurity advisory, warning organizations to be on high alert for ransomware spikes during weekends and holidays. We "have observed an increase in highly impactful ransomware attacks occurring on holidays and weekends — when offices are normally closed — in the United States, as recently as the Fourth of July holiday in 2021," the joint advisory cautions.

The FBI and CISA offer a breakdown of recent actions on Mother's Day, Memorial Day, and the Fourth of July in the brief. Ransomware attacks on those holidays impacted critical infrastructures in the energy sector, food and agricultural sector, and the IT sector. Due to these past issues, "the FBI and CISA encourage all entities to examine their current cybersecurity posture and implement the recommended best practices and mitigations to manage the risk posed by all cyber threats, including ransomware," urges the advisory.

Additionally, CISA has updated its extensive ransomware resources with a "one-stop location, the "Stop Ransomware" website. The new offering combines an amalgam of federal tips and online tools across all industries with specific sector links, preparation guides, education, incident response, and more. Find the new guidance at www.cisa.gov/stopransomware.

Add These 7 Terms to Your Digital Dictionary

Data security incidents continue to be a serious concern for providers and hospitals. Recent studies suggest that the average cost of a breach in 2020 for a healthcare organization was more than $4.6 million (see *Health Information Compliance Alert*, Vol. 21, No. 8).

Understanding the IT terminology and identifying hackers' modus operandi can help your team safeguard systems and bolster security, saving your organization both money and headache. Consider adding these seven additions to your cybersecurity glossary for future reference.

1. Adware: If your work is constantly being interrupted by annoying advertisements popping up while you're accessing research or a website, then you are dealing with adware. Sometimes adware is just a nuisance that flashes or prompts you to download harmless software. However, there is malicious adware, which hackers use to control your browsing history and systems while infecting your devices. If you notice that your computer lags or redirects you to new pages, you may be a victim of an adware hack.

2. Clickjacking: If you've ever gone to click on a link — but then are redirected to click on a different link — you've been clickjacked. "Clickjacking, also known as a 'UI redress attack,'

is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top level page," explains the Open Web Application Security Project (OWASP), a nonprofit foundation that promotes software security, in its online resource.

3. Cyber Hygiene: One way to clean up your cybersecurity and assess threats is by practicing cyber hygiene. In technical terms, "cyber hygiene describes recommended mitigations for the small number of root causes responsible for many cybersecurity incidents," explains the National Institute of Standards and Technology (NIST) in its Computer Security Resource Center (CSRC) guidance. And, by "implementing a few simple practices," organizations "can address these common root causes," NIST says.

4. Indicator of Compromise: After a ransomware attack, you may enlist a forensic investigator to figure out how and when cybercriminals infiltrated your systems. The incident response team will likely search for indicators of compromise (IOCs) among the network and host artifacts, CISA guidance suggests. Furthermore, incident responders will "assess [the] results for further indications of malicious activity to eliminate false positives," explains the agency.

5. Ingress and Egress Traffic: These terms relate to the in-and-out traffic of network communications. For example, when traffic is coming towards you that would be ingress traffic, which refers to all data communications entering your network from an external source. On the other hand, egress traffic is data that originates in your network that you send out externally to other destinations.

6. Rootkit: Cybercriminals use this set of tools to access and take hold of your system at the root level. One of the biggest problems with rootkit attacks is that hackers obtain this "root-level access" covertly, and then remotely control the systems with the malicious software without users realizing it, suggests NIST.

7. Threat Hunting: The best way to stop cyber attacks is to prepare ahead of time, and threat hunting is a great technique to assist with that process. "Threat hunting is a proactive strategy to search for signs of threat actor activity to prevent attacks before they occur or to minimize damage in the event of a successful attack," expounds the FBI and CISA in the advisory. Alert systems, data logging, behavior-focused analytics, and tracking programs are all critical threat hunting tools, according to the FBI and CISA.

Resource: Review the joint advisory at https://us-cert.cisa.gov/sites/default/files/publications/AA21-243A-Ransomware_Awareness_for_Holidays_and_Weekends.pdf.

Reader Questions

Understand What the FHIR® Standard Means

Question:
All the federal policies coming out for health IT reference the FHIR® acronym. We outsource our IT, so no one working directly in our small practice knows exactly what that term means. What does it stand for, how does it impact healthcare, and how does it affect our practice?

Ohio Subscriber

Answer:
There are actually two-related parts to this commonly-used HIT acronym. Health Level Seven International® (HL7®) Fast Healthcare Interoperability Resources (FHIR®), or HL7® FHIR® for short, refers to a set of internationally-accepted standards for the exchange and transmission of data between healthcare providers using an application programming interface (API) to communicate.

Health data "can be exchanged between different computer systems regardless of how it is stored in those systems," according to an HHS Office of the National Coordinator for Health Information Technology (ONC) fact sheet. Plus, "it allows healthcare information, including clinical and administrative data, to be available securely to those who have a need to access it, and to those who have the right to do so for the benefit of a patient receiving care. The standards development organization HL7® (Health Level Seven®3) uses a collaborative approach to develop and upgrade FHIR," ONC explains.

The primary role of HL7® FHIR® is to enhance care coordination between providers. The technology enables more efficient data exchanges using specific APIs that effectively communicate with each other — even when the systems are different and from diverse vendors or software developers.

Since its first draft in 2012 to now, the HL7® FHIR® standard has evolved exponentially, expanding and changing alongside healthcare's IT renaissance, ONC guidance says.

Now: ONC and the Centers for Medicare & Medicaid Services (CMS) released twin rules that addressed provisions and requirements set forth in the 21st Century Cures Act (Cures Act). Both rules focused on improving interoperability and enhancing health information exchanges.

According to the rules, payers such as Medicare Advantage (MA) organizations, Medicaid managed care plans, Qualified Health Plan (QHP) issuers, and others must now offer patients a secure, standards-based API. The agencies will require payers to utilize HL7® FHIR® Release 4.0.1 for APIs.

Currently, physician practices don't have any such requirements, but that may change soon.

Why? COVID pushed more providers to care for patients digitally — and CMS is considering adding the standard requirement to its Quality Payment Program measures and tying it to incentive payments, the Medicare Physician Fee Schedule proposed rule for calendar year (CY) 2022 suggests. Since the agency is "prioritizing digital quality measurement and focusing on health equity" across its broad spectrum of policies, it is issuing a Request for Information (RFI) on this digital transition, "including the use of Fast Healthcare Interoperability Resources (FHIR) in physician quality programs," a CMS fact sheet on the rule says.

▶ Industry Notes

HHS Declares a Public Health Emergency for Hurricane Ida

With the aftermath of Hurricane Ida leaving four states devastated by the storm, the Department of Health and Human Services (HHS) declares public health emergencies (PHEs) to assist with the efforts.

Details: In the first of the two determinations, HHS Secretary **Xavier Becerra** declared a PHE in Louisiana and Mississippi on Aug. 28 with an effective date set retroactively to Aug. 26. For New Jersey and New York, the PHE has an effective date of Sept. 1.

"Hurricane Ida made landfall as an extremely dangerous storm and is carving a path of destruction that poses a significant threat to health and safety," Secretary Becerra said in an Aug. 30 release after declaring the first PHE. "These declarations and waivers help ensure that some of the most vulnerable residents of Louisiana and Mississippi — beneficiaries of Medicare and Medicaid — have continuous access to the care they need in the aftermath of this storm. We stand ready to provide additional public health and medical support to help impacted communities respond andrecover."

The Hurricane Ida PHEs join two already existing PHEs for the COVID-19 pandemic and the opioid crisis.

The HHS Office for Civil Rights (OCR) also issued Hurricane Ida guidance on HIPAA, reminding that during a PHE the HHS Secretary does have the authority to waive certain sanctions and penalties for covered entities (CEs) with 1135 waivers.

Resources: Read the PHE declarations at www.phe.gov/emergency/news/healthactions/phe/Pages/default.aspx. Find the OCR guidance on HIPAA and Hurricane Ida at

www.hhs.gov/sites/default/files/2021-hurricane-ida-hipaa-bulletin.pdf?language=en. Review the HHS release on the storm and additional resources at www.hhs.gov/about/news/2021/08/30/hhs-secretary-becerra-declares-public-health-emergencies-states-louisiana-and-mississippi-due-to-hurricane-ida.html.

Get the Scoop on ONC's 2021 Tech Forum

If you're interested in the feds, take on the future of health IT, then we've got some good news for you.

The HHS Office of the National Coordinator for Health Information Technology (ONC) is offering a two-day virtual conference for interested parties on Sept. 10 and 17 from noon until 5:00 p.m. EST.

The 2021 ONC Tech Forum sessions cover different but related timely topics and are divided into the following four tracks, according to the forum online materials:

» Track 1: Equity Considerations in Health IT
» Track 2: Advances in Health IT Quality and Interoperability
» Track 3: Public Health IT Infrastructure
» Track 4: Health IT: From Care Delivery to Research

With over 2,000 health IT partners participating online, the forum will include "two afternoons of plenary and breakout sessions on a variety of topics at the forefront of health IT," the agency says.

Peruse all the conference details and register at www.healthit.gov/news/events/2021-onc-tech-forum-virtual. TCI

Health Information
COMPLIANCE ALERT

We would love to hear from you. Please send your comments, questions, tips, cases, and suggestions for articles related to *Health Information Compliance Alert* to the Editor indicated below.

Kristin J. Webb-Hollering, BA
kristin.hollering1@aapc.com
Development Editor

Leesa A. Israel, BA, CPC, CUC, CEMC, CPPM, CMBS
leesa.israel@aapc.com
Head of Publishing, Editorial & Technology

The Coding Institute LLC, 2222 Sedwick Road, Durham, NC 27713 Tel: 1-800-508-2582 Fax: (800) 508-2592 E-mail: service@codinginstitute.com

Health Information Compliance Alert is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

Rates: USA: 1 yr. $299. Bulk pricing available upon request. Contact Medallion Specialist Team at medallion@codinginstitute.com. All major credit cards accepted.

This publication has the prior approval of the American Academy of Professional Coders for 0.5 Continuing Education Units. Granting of this approval in no way constitutes endorsement by the Academy of the content. To access each issue's CEU quiz, visit Supercoder.com/ceus and then log in. To request login information, email us at password@supercoder.com

This CEU remains valid for one year from this issue's month.

AAPC CEU APPROVED