



Health Information Compliance Alert

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

In this issue

Business Associates

Evaluate Your BAs' HIPAA IQ Before a Breach Happens **2**
▶ Hint: Understand what OCR means by 'satisfactory assurances.'

Practice Management

See the Latest OSHA Guidelines on COVID-19 **3**
▶ Tip: Ensure patients' privacy and rights are protected, too.

Labor Law

Know the Facts on Mandatory Vaccines Under ADA, Title VII **4**
▶ Critical: Would an unvaccinated person pose a 'direct threat' under the law?

COVID-19 Toolkit

Check Out Online Tools to Bolster Your Vaccination Rollout **5**
▶ Tip: Check specialty orgs for differentiated professional advice.

Reader Question

Prepare Now for Cures Act Compliance Requirements **6**

Enforcement News

OIG Sets Record Straight on Telehealth Fraud Enforcement **7**

and more...

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

Don't Be Fooled by Vendors' 'HIPAA-Compliant' Labels

Tip: Investigate BAs' HIPAA track records.

Many vendors target the healthcare market with promises that their products are HIPAA-compliant. Unfortunately, you cannot buy HIPAA compliance — and these claims won't stop the feds from investigating if your organization has a violation or data breach.

Background: In December, the Federal Trade Commission (FTC) announced a settlement with **SkyMed International, Inc.**, a Scottsdale, Arizona-based firm that sells travel and medical emergency services, for exposing consumers' personal information in a data security breach. After a 2019 complaint, the FTC discovered that SkyMed failed to protect individuals' data, including health information, when an unsecured cloud database exposed 130,000 membership records on the internet. In addition, the FTC found that the organization didn't properly assess its risks "by performing penetration testing and other measures, and failed to monitor its network for unauthorized access," an FTC release says.

Though SkyMed alerted current and former customers that their payment and health information wasn't compromised in the breach, the firm didn't actually review the data nor look into unauthorized access of the database materials, the FTC asserts. "Instead, after confirming that the data was online and publicly accessible, SkyMed deleted the database," the release says.

Here's the Case Clincher

But, on top of risk analysis fails, a data breach, and botched investigation of said incident, SkyMed also duped consumers into believing that its services were HIPAA compliant.

"SkyMed deceived consumers by displaying for nearly five years a 'HIPAA Compliance' seal on every page of its website, which gave the impression that its privacy policies had been reviewed and met" HIPAA security and privacy requirements, the FTC alleges.

Many third-party firms say that their products or tools are "HIPAA compliant," but the Department of Health and Human Services (HHS) and its auxiliary agencies don't certify or endorse vendors' products as HIPAA compliant.

Reminder: "HHS does not endorse or otherwise recognize private organizations' 'certifications' regarding the Security Rule, and such certifications do not absolve covered entities of their legal





obligations under the Security Rule. Moreover, performance of a ‘certification’ by an external organization does not preclude HHS from subsequently finding a security violation,” HHS Office for Civil Rights (OCR) guidance says.

Find Out What ‘HIPAA Compliant’ Means to Your Vendor

It’s important for covered entities (CEs) and their business associates (BAs) to thoroughly vet their third-party partners and vendors before they enter into business with them. This might involve an initial scorecard to test knowledge of the HIPAA basics, followed by a more comprehensive investigation of their compliance practices, breach history, and incident response protocols.

Why? As required by HIPAA, CEs and BAs must secure patients’ protected health information (PHI), and they “would be wise to use caution in evaluating companies that promise ‘HIPAA compliance,’” advises attorney **Shannon Hartsfield**, an executive partner with Holland & Knight LLP in Tallahassee, Florida.

► Business Associates

Evaluate Your BAs’ HIPAA IQ Before a Breach Happens

Hint: Understand what OCR means by ‘satisfactory assurances.’

For covered entities (CEs), one of the most critical aspects of the job is protecting confidential patient information. And that’s why it’s essential that you know whether your business associates (BAs) and vendors really understand the importance of HIPAA compliance before you share protected health information (PHI) with them.

“A lot of customers want to see that characterization, and companies selling their services want to provide it. In my view, because HIPAA compliance is an ongoing process, it would be wise to avoid making representations that attempt to ensure 100 percent compliance,” Hartsfield says.

Tip: Advertisements that claim products are “HIPAA compliant” or “HIPAA certified” should always be questioned.

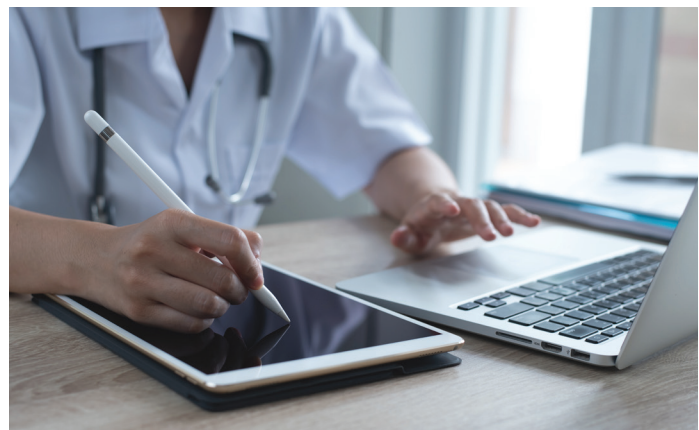
“If a healthcare provider is evaluating a company that says they’re ‘HIPAA compliant,’ it would be important to try to get a full understanding of what the vendor means by that,” Hartsfield says. “And if a vendor says it’s ‘HIPAA compliant,’ you may need to run the other way! Misspelling HIPAA can be a real red flag,” she adds.

End result: According to the proposed settlement, the FTC requires SkyMed to take several actions to correct its compliance issues. Here’s a short sampling of what the proposed settlement entails:

- » Contact the individuals impacted by the data breach.
- » Implement an information security program, including the adoption of a compliance officer, written policies and procedures, and risk analysis and management.
- » Ensure security measures are assessed by a third party.

Another component of the settlement relates to SkyMed’s “HIPAA-compliant” pledge. “The proposed settlement prohibits misrepresentations about how SkyMed secures consumer information, how it responds to data breaches, and whether the company has been endorsed by or participates in any government-sponsored privacy or security program,” notes the FTC release.

Resource: See the case details at www.ftc.gov/system/files/documents/cases/skymed_-_consent_order_ftc_signed.pdf. [tci](#)



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.

Reminder: A BA “is any person or entity that performs a function or activity on behalf of the practice involving the use and/or disclosure of PHI that is not a part of the practice’s staff,” reminds **Kent Moore**, senior strategist for physician payment at the American Academy of Family Physicians.

Additionally, because these BAs have access to your patients’ medical records, they are subject to HIPAA.

Know These Facts on BAs

“HIPAA requires covered entities and business associates to obtain ‘satisfactory assurances’ that their vendors that need access to protected health information will safeguard that information appropriately,” says attorney **Shannon Hartsfield**, an executive partner with Holland & Knight LLP in Tallahassee, Florida.

In the past, the HHS Office for Civil Rights (OCR) “has indicated that companies don’t necessarily need to do much more than obtain a written business associate agreement from the vendor that complies with HIPAA and conduct a risk analysis,” Hartsfield adds.

For example, consider the OCR guidance on cloud services providers (CSPs), Hartsfield suggests. “The HIPAA Rules do not expressly require that a CSP provide documentation of its security practices or otherwise allow a customer to audit its security practices,” according to OCR.

However: As part of the HIPAA Security Rule, CEs and BAs are required to “conduct an ‘accurate and thorough’ analysis of the risks and vulnerabilities to electronic protected health information (ePHI),” Hartsfield reminds. “OCR has indicated that customers may ask vendors for ‘additional assurances of protections for the PHI, such as documentation of safeguards or audits, based on their own risk analysis and risk management or other compliance activities,’” she says.


Remember: Not too long ago, OCR updated its guidance on the direct liability of BAs, clarifying which “party is ultimately responsible for satisfaction of various responsibilities and patient rights,” explains HIPAA expert **Jim Sheldon-Dean**, founder and director of compliance services at Lewis Creek



Systems LLC in Charlotte, Vermont. “Where the BA is not responsible, the hiring entity is.”

Consider asking your BAs these questions to test their understanding of HIPAA compliance before you add them to the payroll:

- » What HIPAA Rules’ safeguards do you employ to protect PHI/ePHI?
- » Is it possible to review your HIPAA-compliance record?
- » Are you willing to enter into a business associate agreement (BAA)?
- » What tools and services do you offer?
- » Do you perform an annual audit and analyze your risks?
- » What kind of vetting do your employees undergo?
- » Do you train staff on HIPAA compliance — and update when regulations change?
- » Do you implement mobile device management?
- » Are you aware of the spike in cybersecurity risks to the healthcare industry?
- » What are your policies, procedures, and protocols for a data breach?
- » Do you have an incident response plan, including a chain of command, in place?

Resource: Review OCR guidance on BAs at www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html. 

► Practice Management

See the Latest OSHA Guidelines on COVID-19

Tip: Ensure patients’ privacy and rights are protected, too.

A recent release offers new advisory guidance from the Occupational Safety and Health Administration (OSHA) with a glimpse at mandatory COVID-19-related requirements to come.

Lowdown: On Jan. 29, OSHA issued a new guidance document, “Protecting Workers: Guidance on Mitigating and Preventing the Spread of COVID-19 in the Workplace.” The guidance aims to “inform employers and workers in most

workplace settings outside of healthcare to help them identify risks of being exposed to and/ or contracting COVID-19 at work and to help them determine appropriate control measures to implement,” OSHA says on its website.

OSHA issued the guidance in response to the “Executive Order on Protecting Worker Health and Safety” signed by President **Biden** on Jan. 21, the day after his inauguration.



Caveat: While providers may be careful to follow Centers for Disease Control and Prevention (CDC) guidance in patient care, they may not be quite as stringent in their back offices and other non-patient-care areas.

OSHA notes that its recommendations in the guidance are “advisory.” However, don’t be surprised to see them turn mandatory soon. The executive order requires OSHA to “consider whether any emergency temporary standards on COVID-19, including with respect to masks in the workplace, are necessary, and if such standards are determined to be necessary, issue them by March 15, 2021.”

“If OSHA moves forward with issuing an emergency temporary standard (ETS), we expect that many of the recommendations in this guidance will become part of the ETS,” say attorneys **Mark Duvall, Jayni Lanham, and Deepti Gage** with law firm Beveridge & Diamond in online analysis.

OSHA, similar to HIPAA, is in the business of protecting people’s health, data, and rights. This new release touches on

► Labor Law

Know the Facts on Mandatory Vaccines Under ADA, Title VII

Critical: Would an unvaccinated person pose a ‘direct threat’ under the law?


If you’re struggling to get your staff vaccinated, you can refer to recent Equal Employment Opportunity Commission (EEOC) guidance around the issue for labor law compliance concerns.

The EEOC recently issued Technical Assistance Questions and Answers regarding vaccinations for its “What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws” guidance document.

several COVID-19 matters and ideas to inform staff about the dangers of the virus while ensuring the workplace is safe.

Consider asking yourself these OSHA-inspired questions as you plan on how to train staff, manage COVID-19 cases among employees, and communicate the protocols — and the dangers — of the virus:

- » Do you have a COVID-19 coordinator on staff?
- » Have you assessed your organization’s risks on employees contracting the virus?
- » What mitigation steps have you taken to ensure workers’ safety?
- » Are your policies and procedures in line with federal health, privacy, and workplace standards?
- » Do you have “reasonable accommodations” to protect older or disabled employees, who are at a higher risk of getting sick?
- » Have you instituted a comprehensive training program that instructs employees on the most recent mandates related to masks, personal protective equipment (PPE), barriers, ventilation, cleaning, and disinfecting?
- » Do you have screening and isolation policies in place for before, during, and after shifts?
- » Are your protocols proactive, encouraging sick employees to stay home without fear of repercussions?
- » Have you enabled an alert system that allows employees to know when a co-worker has come down with COVID-19 while ensuring the sick individual’s privacy and health data are protected?
- » Is your IT enabled to track and report staff cases of COVID-19?
- » Do you have a plan in place that promotes COVID-19 vaccination while not infringing on workers’ rights or choices to *not* get inoculated, too?

Resource: Review the OSHA guidance is at www.osha.gov/coronavirus/safework. 



Key clarification: “The administration of the vaccine is not a medical examination under the ADA,” emphasize attorneys **Dana Stutzman** and **Claire Bailey** with Hall Render. “Because the employer is not seeking medical information from the employee by simply administering the vaccine, the EEOC does not view vaccine administration as a medical examination. But this doesn’t resolve all ADA-related issues for the employer,” the attorneys warn in online analysis.

However, “in the context of mandatory COVID-19 vaccines, the pre-screening questions necessary to safely administer the vaccine are generally subject to the ADA’s standards for disability-related inquiries,” Stutzman and Bailey caution. “Pre-screening questions associated with mandatory vaccines

would satisfy the Business Necessity Standard if the employer has a reasonable belief, based on objective evidence, that an unvaccinated person would pose a ‘direct threat’ to the health or safety of self or others,” they point out.

Bottom line: “Mandatory COVID-19 vaccines (and the pre-screening questions) pass muster under the ADA and Title VII,” the Hall Render attorneys pronounce.

But employers should remember that such requirements may burden an already strained staffing environment, experts point out.

Resource: The EEOC Q&As are at www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws. [TCI](#)

► COVID-19 Toolkit

Check Out Online Tools to Bolster Your Vaccination Rollout

Tip: Check specialty orgs for differentiated professional advice.

Whether you’re creating a COVID-19 vaccination training template for staff or assisting patients with vaccine-related issues, there’s a myriad of online tools and technology available.

Take a look at five top resources for vaccine administration planning, training, and IT:

1. ONC: If you’re looking for a plethora of helpful links all in one place, then the HHS Office of the National Coordinator for Information Technology (ONC) COVID-19 response page is the ticket. The nation’s health IT agency offers insight and resources on: data collecting and reporting; surveillance and cybersecurity; lab testing; outcome reporting and tracking; interoperability; and telehealth.

“Health IT now plays a crucial role in the collecting and reporting of COVID-19 data. Additionally, electronic health information exchange can facilitate effective strategies to

combat COVID-19,” ONC says in its guidance. Examine the various options at www.healthit.gov/coronavirus.

2. Medicare: Several Centers for Medicare & Medicaid Services (CMS) toolkits offer guidance for healthcare providers ramping up their vaccination plans. “These resources are designed to increase the number of providers that can administer the vaccine and ensure adequate reimbursement for administering the vaccine in Medicare,” CMS says on its vaccine hub.

The agency toolkits provide Medicare-specific COVID-19 vaccination guidance on: enrollment and billing for shot administration; coding, billing, and reimbursement for COVID-19 shots; beneficiary incentives; quality reporting; SNF enforcement discretion for pharmacy immunizers; and COVID-19 therapies and subsequent add-on payments. Access the Medicare tools at www.cms.gov/covidvax-provider.





3. CDC: The Centers for Disease Control and Prevention (CDC) offers an array of vaccination information toolkits, including ones for clinicians, essential workers, and community-based organizations, at www.cdc.gov/vaccines/covid-19/toolkits/index.html. The kits aim to help you “build confidence about COVID-19 vaccination among your healthcare teams ... and staff,” the CDC says.

Plus: On a broader scale, the CDC’s online guidance for immunizations offers overviews on pricing, contracts, laws, and IT. See details at www.cdc.gov/vaccines/imz-managers/index.html.

4. Clinician organizations: Many professional groups have created guides and reference materials on the COVID-19 vaccines. Two of the biggest, the AMA and the American Nurses Association (ANA), offer clinicians guidance on shot administration, but also patient care, ethics, mental health, health equity, liability, staff-related issues, IT, and more. You can find the AMA tools and resources at www.ama-assn.org/delivering-care/public-health/ama-covid-19-guides-health-care-professionals and the ANA guidance at www.nursingworld.com.

[org/practice-policy/work-environment/health-safety/disaster-preparedness/coronavirus](https://www.codinginstitute.com/practice-policy/work-environment/health-safety/disaster-preparedness/coronavirus).

Tip: Specialists may want to check out pertinent professional organizations for specialty-focused assistance. As a specialist, you may not be part of the COVID-19 vaccination rollout — but, that doesn’t mean your patients won’t ask questions or need clinical advice. This is especially true if you care for patients with chronic diseases who need your medical input before deciding on vaccination.

5. FDA: The U.S. Food and Drug Administration (FDA) delves deeply into the nuances of the COVID-19 vaccines with scientific and health perspectives to allay provider, patient, and industry concerns. The guidance includes a mix of fact sheets, FAQs, videos, and more on topics like vaccine basics, research and future vaccines, the emergency use authorization (EUA) process, and healthcare tips. Review the FDA guidance at www.fda.gov/emergency-preparedness-and-response/coronavirus-disease-2019-covid-19/covid-19-vaccines.

Bonus: The FDA fact sheets on the Pfizer-BioNTech COVID-19 vaccine, the Moderna COVID-19 vaccine, and the Janssen COVID-19 vaccine are available for both providers and recipients/caregivers. The offering for healthcare providers administering the vaccine has been translated into six different languages while the patient guidance is available in 27 different languages.

Reminder: Though the **Biden** administration recommends how the vaccines should be dispensed and administered, those final decisions are up to the states — and each one is handling it differently. State tools vary, but most include vaccine management and registration advice, including dashboards with modules, FAQs, patient engagement tips, graphics, inventory, IT assistance, and facility-specific insight.

Check with your individual state to see available resources. [TCI](#)

► Reader Question

Prepare Now for Cures Act Compliance Requirements

Question:

We haven’t seen any new updates on the 21st Century Cures Act compliance deadlines under the Biden administration. Have we missed them or are there any new extensions?

New Hampshire Subscriber

Answer:

No. Despite industry organizations urging the feds to extend the implementation timeline, the first compliance date has not been altered for some standards and is fast approaching.

Refresher: In May 2020, the HHS Office of the National Coordinator for Health Information Technology (ONC) published a final rule in the *Federal Register* that followed through on long-promised



changes to health IT, interoperability, and information blocking, mandated by the 21st Century Cures Act. That final rule carried a compliance due date of Nov. 2, 2020.

Next: In October 2020, ONC announced an extension in an effort to ease providers' implementation burden during the COVID-19 pandemic. ONC "released an interim final rule with comment period that extends the compliance dates and timeframes necessary to meet certain requirements related to information blocking and Conditions and Maintenance of

Certification (CoC/MoC) requirements," an HHS release said of the interim final rule published in the *Federal Register*.

Now: According to ONC guidance, there are specific provisions with a start date of April 5. Those include compliance requirements for Condition of Certification (CoC) for information blocking, assurances, and application programming interfaces (APIs), guidance suggests.

Resource: Review the start dates, definitions, requirements, and more at www.healthit.gov/curesrule/. 

► Enforcement News

OIG Sets Record Straight on Telehealth Fraud Enforcement

If you've noticed a spike in telehealth fraud talk from the feds, you're not alone. However, the HHS Office of Inspector General (OIG) chief wants to clarify that enforcement of "telefraud" and oversight of telehealth services used during COVID-19 are not the same.

Details: From the onset of the pandemic, OIG in coordination with other federal healthcare agencies addressed the critical need for telehealth services in the industry, indicates **Christi A. Grimm**, OIG Principal Deputy Inspector General in a release.

"As we observed in recent rulemaking, OIG recognizes the promise that telehealth and other digital health technologies have for improving care coordination and health outcomes," Grimm says. However, "it is important that new policies and technologies with potential to improve care and enhance convenience achieve these goals and are not compromised by fraud, abuse, or misuse."

That's why OIG ramped up its significant oversight and began auditing telehealth services used during the public health emergency (PHE) across a variety of federal health programs.



Caveat: Parallel to OIG's spotlight on telehealth services, the agency has also seen an escalation of "telefraud" cases, according to the brief.

"OIG has conducted several large investigations of fraud schemes that inappropriately leveraged the reach of telemarketing schemes in combination with unscrupulous doctors conducting sham remote visits to increase the size and scale of the perpetrator's criminal operations," Grimm relates. She further clarifies that though this fraud did involve telehealth services, the fraudulent billing was for items rather than the visit.

Read OIG's release at https://oig.hhs.gov/coronavirus/letter-grimm-02262021.asp?utm_source=oig-covid-portal&utm_medium=oig-news&utm_campaign=oig-grimm-letter-02262021.

Feds Declare PHE for Texas After Winter Mayhem

As with past natural disasters and the COVID-19 pandemic, Centers for Medicare & Medicaid Services (CMS) officials reassured Texas providers they can count on the feds to help after a winter storm ravaged the state.

On Feb. 17, HHS Acting Secretary **Norris Cochran** declared a public health emergency (PHE) for Texas after the spate of winter storms. "This declaration follows President **Biden's** emergency declaration for the state of Texas" and allows CMS "to give healthcare providers and suppliers greater flexibility in meeting emergency health needs in disasters," an HHS release said on the declaration.

The waivers and flexibilities associated with the PHE are retroactive to Feb. 11, CMS indicates.

See more information at www.cms.gov/about-cms/emergency-preparedness-response-operations/current-emergencies/current-non-covid-emergencies.

Industry Group Advocates for State-Aligned Privacy Regs

With the aim of encouraging more discourse on a national privacy law, *Consumer Reports* published a legislative proposal titled the Model State Privacy Act.



The advocacy group’s manifesto promotes reform and better laws to protect consumers’ privacy and rights.

“This lack of legal protections is particularly frustrating because privacy is a basic human right, enshrined in American jurisprudence and in nearly a dozen state constitutions. While there are federal laws that provide certain protections for financial and some health data, there is no comprehensive federal privacy law granting consumers baseline privacy and security protections,” the brief says.

Access the Model State Privacy Act at https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf.

Submit 2020 Medicare PI Data ASAP

If you haven’t submitted your Promoting Interoperability (PI) Program data for 2020 yet, the deadline is around the bend.

Heads up: “The Centers for Medicare & Medicaid Services (CMS) reminds all Medicare Promoting Interoperability Program participants that the deadline to submit 2020 data is April 1, 2021 at 11:59 PM ET,” an alert says.

PI participants can both register and attest through CMS’ quality portal at <https://qualitynet.cms.gov>.

Medicare Eligible Hospitals and Critical Access Hospitals (CAHs) can use the portal to send their data while “Medicaid Eligible Professionals (EPs), Eligible Hospitals, CAHs should follow the requirements of their State Medicaid agencies to submit their meaningful use attestation,” CMS notes.

Dual-Eligible Hospitals and CAHs demonstrating meaningful use should also submit through the CMS’ quality portal, when they qualify for both the Medicare and Medicaid PI Programs.

Check out the PI guidance at www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms. [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
Development Editor
kristin.hollering1@aapc.com

Leesa A. Israel, BA, CPC, CUC, CEMC, CPPM, CMBS
leesai@supercoder.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.

CPT® codes, descriptions, and material only are copyright 2020 American Medical Association. All rights reserved. No fee schedules, basic units, relative value units, or related listings are included in CPT®. The AMA assumes no liability for the data contained herein. Applicable FARS/DFARS restrictions apply to government use.

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.



The Coding Institute also publishes the following specialty content both online and in print. Call us for a free sample of any or all of the specialties below:

- Anesthesia
- Cardiology
- Emergency Medicine
- Evaluation & Management
- Gastroenterology
- General Surgery
- ICD-10 Coding
- Neurology & Pain Management
- Neurosurgery
- Ob-Gyn
- Ophthalmology and Optometry
- Orthopedics
- Otolaryngology
- Part B (Multispecialty)
- Pathology/Lab
- Pediatrics
- Podiatry
- Practice Management
- Primary Care
- Pulmonology
- Radiology
- Urology

Call us and mention your customer number for a special price, free trial, or just to find out more about SuperCoder – the complete online medical coding solution.