

# Health Information Compliance Alert

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

March 2017, Vol. 17, No. 3 (Pages 17-24)

## In this issue

Safeguard Yourself, But Don't Let Your Arrangements Impede Data Sharing **p18**

▶ If you're dealing with complex information, make sure you're covered.

### Telemedicine

Ride the Telehealth Wave to Revenue Reward **p19**

▶ With the right tools and utilization, telemedicine boosts both workflow and income.

Does Convenience Trump Utilization Cost in Telehealth? **p21**

▶ As the delivery of virtual care increases, a study ponders whether it's worth the cost.

### Enforcement News

House Unveils Its Opus to Replace the ACA **p21**

### Clip And Save

Take a Look at Some Recent Changes for Telemedicine from CMS **p22**

▶ New guidance defines the role of modifier 95.

*We welcome your comments & suggestions!*

E-mail **Jan Milliman**, Editorial Director, at:  
[janm@codinginstitute.com](mailto:janm@codinginstitute.com)

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

## Case Study

### Design Your HIPAA Plan to Protect Against Threats — Both External and Internal

Make sure your business associates understand the exit rules when employees leave.

What do small practices, big hospitals, multi-specialty clinics, physical therapy firms, DME businesses, and other healthcare entities have in common? They all have employees come and go. And if you don't have an exit strategy built into your HIPAA plan, then electronic protected health information (ePHI) can be compromised from the threat within.

**Background:** As a recent settlement indicates, one dangling thread can cause the whole operation to unravel.

Memorial Health Systems (MHS) is a non-profit, operating six hospitals, an urgent care center, a nursing home, and a variety of ancillary healthcare facilities in South Florida, in addition to having an Organized Health Care Arrangement (OHCA) with several physicians' offices. Due to a lack of clear-cut employee review procedures, MHS suffered the loss of ePHI on separate occasions that led to a \$5.5 million settlement for HIPAA violations, a joint U.S. Department of Health and Human Services (HHS) and Office of Civil Rights (OCR) press release from Feb. 16, 2017 says.

**The facts:** Here's an outline of how MHS violated HIPAA from the HHS-OCR release:

- » Ignored the risks of users and affiliated physicians' office users between 2007 and 2012 who had access to ePHI, failing to properly review terminated users' rights under HIPAA despite the advice from risk analysis to do so.
- » Failed to notice the daily access of ePHI by a terminated employee whose credentials were not revoked, resulting in the loss of ePHI for over 80,000 individuals from 2011 to 2012.
- » Reported the loss of "protected health information (PHI) of 115,143 individuals, which had been impermissibly accessed by its employees and impermissibly disclosed to affiliated physician office staff."

### Was the Organization's Size a Factor?

Sometimes a small practice can be too trusting while a big healthcare group can be too busy to notice the day-to-day workings of its employees past and present. But it can be hard to justify these types of excuses with so many resources out there

to help avoid HIPAA pitfalls. “While I think being busy or the ‘that won’t ever happen to me’ logic may come into play,” says attorney **Kathleen D. Kenney, Esq.**, of Polsinelli LLP in Chicago. “Ultimately, I think this issue, like many HIPAA issues that arise, stems from a failure to implement processes and ensure checks and balances are in place when it comes to security.”

## Analyze Then Manage Your Risk

To avoid issues like those that tripped up MHS, your practice must first assess compliance shortcomings — from reining in reception desk banter to multi-factor authentication on your mobile devices. But you need to scrutinize your findings in order to fully implement and

## Safeguard Yourself, But Don’t Let Your Arrangements Impede Data Sharing

If you’re dealing with complex information, make sure you’re covered.

As the Memorial Health System breach highlights, the more diverse the affiliations, the more in-depth the controls need to be. And when you have this kind of integrated relationship with a mix of hospitals, physicians’ offices, business associates and more — you need to protect yourself, your patients, and the data you are sharing.

An Organized Health Care Arrangement or OHCA provides relief and aims to assist with the coordination of care, protecting the separate covered entities and increasing workflow across the different healthcare spectrums.

**OHCA defined:** An Organized Health Care Arrangement (OHCA) allows the different covered entities in the separate clinically integrated healthcare settings to work together under HIPAA, AHIMA suggests in its guidance on compliance arrangements. “The HIPAA privacy rule also permits providers that typically provide healthcare to a common set of patients to designate themselves as an OHCA for purposes of HIPAA,” AHIMA explains. See the AHIMA guidance here: <http://library.ahima.org/doc?oid=60011#.WMLT4BiZNAY>.

**More info:** “By participating in an OHCA arrangement under HIPAA, legally separate covered entities without common ownership or control that are clinically or operationally integrated can more easily share

appropriate and necessary information,” says attorney **Kathleen D. Kenney, Esq.**, of Polsinelli LLP in Chicago. However, those involved need to remember that they still need to follow compliance standards. “The obligation under HIPAA to ensure access and audit controls are in place for any user that accesses a covered entity’s system containing ePHI does not change because of an OHCA arrangement,” Kenney points out.

**Think ahead:** Many providers complain that mandates and administration get in the way of helping patients. But, it’s important to note that safeguarding your practice upfront can help you avoid the hassles later on. As more and more complex information is passed from one provider to the next via technologically-implemented devices — particularly within a multi-layered organization similar to Memorial Health System — it is easy to see how ePHI can be lost. Having HIPAA controls in place ahead of time can help prevent such problems.

**Tip:** The feds don’t “want HIPAA to serve as a barrier for data sharing arrangements — but it’s important for organizations to evaluate HIPAA compliance as they begin to do more with their data,” advises Kenney. “Thinking through the regulatory issues first and putting in place checks and balances allows covered entities to ensure safeguards and protocol do not get overlooked along the way.” □

*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 ©2017 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.

manage a working HIPAA system. “We regularly see organizations with policies and procedures in place but they have stopped there,” Kenney says.

**Federal clarification:** Your assessment should look at how a breach would “negatively impact” your practice’s ePHI, suggests the HHS in its Q-and-A on the difference between risk analysis and risk management. When you analyze, you “consider all relevant losses that would be expected if the security measures were not in place,” HHS notes. Management of that risk involves the way your practice implements HIPAA controls from the garnered information. Read the HHS Q-and-A here: <https://www.hhs.gov/hipaa/for-professionals/faq/2013/what-is-the-difference-between-risk-analysis-and%20risk-management-in-the-security-rule/index.html>.

“The implementation piece of HIPAA compliance is integral to breach avoidance,” reminds Kenney. “OCR wants to see more than just documents on a shelf so taking the time to evaluate and carry out processes is key.”

**HIPAA go-to list:** After you educate your current staff on insider threats, consider these compliance dos and don’ts for future employees and after employees move on:

- » Do a comprehensive background check on future employees in regard to compliance issues.
- » Do provide up-to-date materials on the changing compliance regulations for your staff.
- » Don’t forget to monitor your network and controls with tools that check log-on access and irregularities.
- » Don’t assume the “one-password-fits-all” mentality. Change your passwords often and implement multi-factor authentication.
- » Do remember that the majority of breaches are caused from within an organization through employee oversight, accident, and theft of ePHI.

**Reminder:** MHS paid heavily despite its risk analysis due mostly to the lack of utilizing the data and ensuring only authorized users had access to the ePHI. “As this case shows, a lack of access controls and regular review of audit logs helps hackers or malevolent insiders to cover their electronic tracks, making it difficult for covered entities and business associates to not only recover from breaches, but to prevent them before they happen,” said **Robinsue Frohboese**, OCR acting director in the release. □

## Telemedicine

# Ride the Telehealth Wave to Revenue Reward

With the right tools and utilization, telemedicine boosts both workflow and income.

Advancements in technology and the digitization of practice management have improved healthcare in ways most never dreamed possible.

Telehealth falls into this category as it allows providers to virtually interact with their patients, improving the delivery of care for those unable to come into the office. But connecting with patients remotely can be a compliance headache if your tools aren’t user-friendly or lack the proper security protocols to ensure the process is both safe and compliant.

### Get the Scoop

Telemedicine can be a boon for folks left behind by hospital consolidations and the lack of medical resources in rural areas of the country, but it is actually more

than just a replacement of an office visit and it’s not for everyone. Both the provider and the patient have to be on board, and depending on the type of telemedicine you’re practicing, the upfront hardware cost can be high.

**Reasoning:** There are many factors that go into the successful utilization of telemedicine at your practice, but the primary one is educating your staff on the how and why of telehealth. “Hospitals, healthcare systems, and practices should first understand the value of a telehealth solution,” says **Lee Horner**, president of telehealth at Stratus Video in Clearwater, Fla. “The ideal telehealth solution works with existing workflows and helps to automate your established processes.”

**Fundamentals:** Telemedicine covers more than just the virtual consultation that most people think of when

*(Continued on next page)*

they hear “telehealth.” It is actually broken down into three distinct areas and involves real-time online visits, recorded and saved interactions, and long-term observation via telehealth tools:

- » **Store-and-forward data collection** allows the physician to share data and the recorded visit with other providers, usually a specialist, who may be needed to remedy the patient’s diagnosis.
- » **Remote patient monitoring** is extremely helpful with chronic conditions and lets the provider check-in with the patient and monitor reports and changes in his health with the right equipment.
- » **Synchronous telehealth** refers to the real-time virtual delivery of telemedicine using audio and video technologies to perform the visit.

## Here’s the Rub

Telemedicine can be an incredibly useful tool, but if you don’t keep HIPAA regulations in mind, you can get yourself in hot water. “HIPAA compliance is a must-have for any telehealth solution,” advises Horner. “Because hospitals and healthcare systems are dealing with electronic protected health information (ePHI), any telehealth system must first and foremost ensure that all the required physical, network, and process security measures are in place and followed.”

**Consider this:** Telemedicine delivery is dependent on mobile devices and software that allows you to talk with your patient one-to-one during the virtual consultation, so it’s no surprise that following the HIPAA Security rule is essential.

To avoid problems, you need to include this type of communication in your compliance planning, ensuring that the office staff knows the rules of engagement. “I think the challenge comes more with Security Rule compliance than Privacy Rule compliance,” says attorney **Michael D. Bossenbroek, Esq.**, of Wachler & Associates, P.C. in Royal Oak, Mich. “However, there is what I would refer to as ‘low hanging fruit’ or basic HIPAA compliance issues that the OCR has repeatedly identified and that a practice could address without much difficulty.”

**Remember:** A breach can happen with telehealth services just like it can with a patient portal in an EHR, a front office breakdown, or a misaddressed postcard. You need to outline from the beginning

what’s at stake and enlist a reputable and experienced telehealth vendor.

As you go about setting up your system, ask yourself these questions from the HIPAA Security Rule:

- » Who’s authorized to access ePHI through telemedicine in the office?
- » Are the communications’ materials and hardware safe, secure, and HIPAA-ready to protect the integrity of ePHI?
- » How are you going to monitor the telehealth solutions in your practice?
- » Who is going to assess and analyze the risk to protect against a breach?

## Think About What Your Practice Needs

For you to successfully offer telehealth services to your patients, you have to invest in the right applications, software, and hardware for your practice.

**Nuts and bolts:** Whether you are a telehealth novice or have been engaged in telemedicine for a while, understand that the best system is one that enhances your patients’ care not hinders it.

It’s important to note that both physicians and staff work better when they are able to use devices they are familiar with when adopting new telehealth technologies, suggests Horner. “This will help drive quick adoption and ongoing usage as it will not require significant behavioral change from physicians and staff,” he adds. “Also, the ideal telehealth solution should be able to leverage the investments an organization has already made in personal devices and technology.”

**Apps matter:** Seek out a vendor with telehealth street cred that understands HIPAA and business associate agreements (BAAs). Their programs should be easily adaptable to your office tech and translatable to your patients. “Physicians and staff will appreciate being able to use everyday devices (such as smartphones, tablets, etc.) with a HIPAA-compliant technology that delivers on convenience and optimizes patient care,” Horner says.

**Tip:** Function and ease-of-use are essential to telehealth implementations, especially when dealing with critical care crises. “Intuitive solutions allow staff to react quickly and immediately reach needed specialists,” explains Horner.

For more information on telehealth and Stratus Video, visit <https://www.stratusvideo.com>. □

## Does Convenience Trump Utilization Cost in Telehealth?

As the delivery of virtual care increases, a study ponders whether it's worth the cost.

Telehealth is ramping up to be a major player in the quality care game as new technologies allow for increased patient access and revenue. But a new *Health Affairs* study suggests that though it's touted as a cost-saving service, hidden expenses can arise and impact implementation.

The investigation led by a RAND Corporation policy researcher and a Harvard professor found that “increased convenience may tap into unmet demand for healthcare, and new utilization may increase overall healthcare spending,” according to the study's abstract. See the abstract here: <http://content.healthaffairs.org/content/36/3/485.abstract?=&right>.

**Stats:** The researchers examined over 300,000 patients from 2011 to 2013, using commercial data on telehealth services for acute respiratory illnesses to see if the convenience of the service was equal to the cost of the implementation. “Twelve percent of direct-to-consumer telehealth visits replaced visits to other providers, and 88 percent represented new utilization,” the abstract said. However, “net annual spending on acute respiratory illness increased \$45 per telehealth user.”

**Reminder:** Make sure you know your payer's policy on telemedicine and HIPAA guidelines before you report any telemedicine codes. Keep in mind that each states' Medicaid guidelines for telemedicine will be unique from each other and different from Medicare national guidelines, so check your specific state's Medicaid guidelines as well. As practices begin to use telemedicine more commonly, many regulators are pushing for tighter telemedicine guidelines and this may impact the cost to you as well. □

### Enforcement News

## House Unveils Its Opus to Replace the ACA

House Republicans made good on their promise to put the Affordable Care Act — also known as Obamacare — to bed this week with sweeping changes. They premiered the new American Health Care Act, which eliminates insurance requirements and drastically reforms Medicaid but does keep some of the most popular parts of the ACA — the ban on denying insurance coverage to people with pre-existing conditions and on lifetime coverage caps, and the provision allowing people to remain on their parents' insurance until age 26.

**What's In:** If you have a pre-existing condition, the new plan will still cover it. The same goes for coverage up until age 26 under your parents' insurance. Insurers still can't set limits on coverage and must still provide “10 essential health benefits, including maternity care and preventive services,” a *New York Times* article from March 6 said.

**What's Out:** Employers are no longer required to offer coverage for their employees, and people are no longer required to get insurance if they can't afford it. The

popular cost-sharing subsidy that helps fill in the gaps with co-pays and deductibles will be phased out by 2020.

*(Continued on next page)*

## We Want to Hear From You

Tell us what you think about *Health Information Compliance Alert*

- What do you like?
- What topics would you like to see us cover?
- What can we improve on?

We'd love to hear from you.

Please email **Kristin J Webb-Hollering** at [kristinwh@codinginstitute.com](mailto:kristinwh@codinginstitute.com)

## Clip And Save

## Take a Look at Some Recent Changes for Telemedicine from CMS

## New guidance defines the role of modifier 95.

With its push toward providing value-based care under MACRA, it's no surprise that CMS has offered guidance and new options to promote advancements in telehealth.

**Backtrack:** CMS invested in telehealth with new code options in its 2017 Medicare Physician Fee Schedule (MPFS) Final Rule, which moved the practice of telemedicine beyond the traditional venues to more alternative settings for enhanced patient care. The highlights include new CPT® codes for end-stage renal disease (ESRD)-related services for dialysis (90967-90970); advanced care planning (99497-99498); and critical care consultations (G0508-G0509). The new options went live on Jan. 1, 2017.

**Choices:** In the 2017 AMA CPT® manual, Appendix P lists the 79 codes you can use to report synchronous (real-time) telemedicine services. Also new for 2017, CPT® identifies the appropriate telemedicine codes with a star (★) symbol next to the code in the code set.

**POS update:** CMS also created a new place of service (POS) code for telemedicine: POS 02 (*Telehealth: The location where health services and health related services are provided or received, through a telecommunication system*), according to a *MLN Matters* article released on Aug. 12, 2016. Read the article here: [www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNMattersArticles/Downloads/MM9726.pdf](http://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNMattersArticles/Downloads/MM9726.pdf).

**New choices:** This year, CPT® has given you modifier 95 (*Synchronous telemedicine service rendered via a real-time interactive audio and video*

*telecommunications system*) to report telemedicine services your physician provides via real-time, interactive audiovisual telecommunications.

Don't forget to append either modifier GT (*Via interactive audio and video telecommunication systems*) or GQ (*Via asynchronous telecommunications system*) to your CPT® or HCPCS code when you list POS 02 for telemedicine on your claim — if you don't, expect a denial from your MAC.

**Why modifiers?** “It's important for the payers to know if the patient was physically in the office or seen via telemedicine,” says **Suzan Hauptman, CPC, CEMC, CEDC**, senior principal of ACE Med group in Pittsburgh, Pa. “Because the codes are the same regardless of physical location, the 95 modifier tells this part of the story.”

As for knowing which modifier to choose for real-time services, “practices should check with their respective payers on telemedicine coverage policies and the use of the appropriate modifier — 95 or GT,” says **Mary I Falbo, MBA, CPC**, CEO of Millennium Healthcare Consulting, Inc.

**Reminder:** Telemedicine services must meet a certain set of rules to be covered for Part B beneficiaries and questions should be directed to your carrier for clarification. For a list of the current approved telemedicine services approved by Medicare, visit <https://www.cms.gov/Medicare/Medicare-General-Information/Telehealth/Telehealth-Codes.html>. □

(Continued from previous page)

Read the full text of the bill here: <https://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/documents/AmericanHealthCareAct.pdf>.

**HHS response:** “On behalf of the Trump Administration, I am writing in support of the reconciliation recommendations recently released for consideration by your Committees. Together, they align with the

President's goal of rescuing Americans from the failures of the Affordable Care Act,” said **Thomas E. Price, MD**, HHS Secretary in an open letter to **Greg Walden**, House Committee on Energy & Commerce Chairman and **Kevin Brady**, House Committee on Ways & Means Chairman.

Price's endorsement comes as no surprise — he was a vocal critic of the ACA since its inception as the former House Rep from Georgia. “These proposals offer patient-centered solutions that will provide all

Americans with access to affordable, quality healthcare, promote innovation, and offer peace of mind for those with pre-existing conditions,” Price said. Read the letter in its entirety here: <https://www.hhs.gov/about/news/2017/03/07/secretary-price-supports-house-efforts-repeal-and-replace-obamacare.html>.

**AMA rebuttal:** As medical groups across the nation weighed in against the new legislation, the American Medical Association (AMA), a supporter of Secretary Price’s nomination, advised the feds to go slowly because this swift decision, which it called “critically flawed,” could have far-reaching effects, endangering the health and welfare of Americans.

“As you consider this legislation over the coming days and weeks, we hope that you will keep utmost in your mind the potentially life-altering impact your decisions will have on millions of Americans who may see their public, individual or even employer-provided health care coverage changed or eliminated,” said **James L. Madara, MD**, CEO of the American Medical Association (AMA) in a letter to the two House committee leaders.

With many of the alterations aimed at Medicaid and the promise to push much of the responsibility on the states for implementation of the new plan, the jury is out on how quickly and at what cost to taxpayers the transition from the ACA to the American Health Care Act will proceed.

**Resource:** To take a look at the *New York Times* article, <https://www.nytimes.com/interactive/2017/03/06/us/politics/repUBLICAN-obamacare-replacement.html>.

## OCR Says US-CERT’s Got Your Back

If you haven’t signed up for the monthly *OCR Cyber Awareness Newsletter*, now is the time to hit that listserv.

In its most recent issue, the cyber watchdog outlined what the United States Computer Emergency Readiness Team (US-CERT) does and how it can help providers. The branch, one of four, falls under the National Cybersecurity and Communications Integration Center (NCCIC) in Homeland Security.

“US-CERT is in a unique position to inform covered entities and business associates about their cybersecurity efforts as well as benefit from information sharing when a covered entity or business associate experiences a cybersecurity incident,” says the February 2017 newsletter. “Covered entities should report to US-CERT

any suspicious activity, including cybersecurity incidents, cyber threat indicators and defensive measures, phishing incidents, malware, and software vulnerabilities.”

In this edition, US-CERT explains the who, what, and when of the Grizzly Steppe Activity, responsible for the Russian malware infiltration that impacted the U.S. election last year and analyzes how spear phishing attacks can impact even the strongest HIPAA plans.

For a closer look at last month’s *OCR Cyber Awareness Newsletter*, visit <https://www.hhs.gov/sites/default/files/february-2017-ocr-cyber-awareness-newsletter.pdf?language=es>.

## CMS Reorganizes eQOM Guidance with MACRA Updates

With MACRA up and running, changes have come quickly as CMS scrambles to switch over from fee-for-service to the new Quality Payment Program. One of the major players on the cutting room floor — Meaningful Use — disappeared for most Medicare providers on March 13, 2017, which marked the last day to attest measures for 2016. Advancing Care Information replaced Meaningful Use as Medicare’s new EHR incentive program on Jan. 1, 2017.

CMS updated its Electronic Clinical Quality Measures (eCQMS) guidance to keep eligible clinicians in the loop for 2017 reporting. “In an effort to align the eCQMs used in CMS quality reporting programs with the goals of CMS and the Department of Health and Human Services, the National Quality Strategy (NQS), and recommendations from the Health Information Technology Policy Committee, each eCQM has been assessed against six domains based on the six priorities of the NQS,” the CMS eCQM guidance said. “This revised table removes the previous Meaningful Use domains and now aligns with the domains listed in the Merit-based Incentive Payment System (MIPS) and Alternative Payment Model (APM) Incentive under the Quality Payment Program.”

Unfortunately, if you missed the last MU reporting deadline, you will be assessed penalties. Here is a link to the 2016 program requirements: <https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/2016ProgramRequirements.html>.

To take a look at the changes, visit [https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/eCQM\\_2016EPEC\\_MeasuresTable.pdf](https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/eCQM_2016EPEC_MeasuresTable.pdf). □

# Health Information

## COMPLIANCE ALERT

**Leesa Israel, CPC, CUC, CMBS**

leesai@codinginstitute.com  
 Director, SuperCoder.com From The Coding Institute

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**

Editor  
 kristinwh@codinginstitute.com

**Jan Milliman, MA, HCS-D, COS-C**

janm@codinginstitute.com  
 Editorial Director

**Suzanne Burmeister, BA, M.Phil., CPC, COBGC,**

suzanneb@codinginstitute.com  
 Managing Editor

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 2016 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 1-800-508-2582 for a free sample of any or all of the specialties below:

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

Call us (800-508-2582) 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.

## Order or Renew Your Subscription!

Yes! Start/Renew my one-year subscription (12 issues) to *Health Information Compliance Alert*

- Print & Online - \$399 (Special Renewal price for active subscribers - **\$299 only!**)
- Print only - \$299
- Online only - \$199

Name \_\_\_\_\_

Title \_\_\_\_\_

Company \_\_\_\_\_

Address \_\_\_\_\_

City, State, ZIP \_\_\_\_\_

Phone \_\_\_\_\_

Fax \_\_\_\_\_

E-mail \_\_\_\_\_

\* Must provide e-mail address if you choose "online" or "both" option to receive issue notifications  
 To help us serve you better, please provide all requested information

**PAYMENT OPTIONS**

Charge my:  MasterCard  VISA  
 AMEX  Discover

Card # \_\_\_\_\_

Exp. Date: \_\_\_\_ / \_\_\_\_ / \_\_\_\_

Signature: \_\_\_\_\_

Check enclosed  
 (Payable to *The Coding Institute*)

Bill me (please add \$15 processing fee for all bill me orders)

***Health Information Compliance Alert***

The Coding Institute  
 PO Box 933729  
 Atlanta, GA 31193-3729  
 Call 1-800-508-2582  
 Fax 1-800-508-2592  
 E-mail: service@codinginstitute.com

Promo Code: P37RAA01



SuperCoder is a property of CodingInstitute.com