

# Health Information Compliance Alert

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

May 2019, Vol. 19, No. 5 (Pages 33-40)

## In this issue

### Telemedicine

Master Telemedicine and  
Telehealth Coding With  
3 Key Tips

p34

► Plus: Find out why telehealth  
and telemedicine aren't the same.

### HIPAA

Do CMP Rollbacks Signal  
Major Changes for HIPAA  
Enforcement?

p36

► Hint: Risk management  
is even more important now.

### Reader Questions

Review This Password Guidance  
Before Your Next Update

p38

What Happened to the HIPAA  
Audit Program?

p38

### Enforcement News

Public Gets More Time  
to Comment on  
Interoperability Rules

p39

Hospitals Increasingly Use  
EHR Data to Improve Care

p39

Tennessee Company Agrees  
to Pay \$3 Million to Settle  
HIPAA Violations

p39

*We welcome your  
comments & suggestions!*

E-mail **Kristin J. Webb-Hollering**  
Editor-in-Chief, at:  
[kristinwh@codinginstitute.com](mailto:kristinwh@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

### Feds Indict 24 Individuals for Telemedicine Fraud

Prescribing DME or drugs via telemedicine? Document it — thoroughly.

If your practice is one of many jumping on the telemedicine train, your patients are lucky to have the electronic option of a clinician's care. However, the convenience of offering clinical services electronically has its drawbacks. In fact, a recent case suggests the feds aren't playing any games when it comes to proving medical necessity for telemedicine claims.

**Context:** Last month, the **Department of Justice (DOJ)**, in collaboration with the **Department of Health and Human Services (HHS)**, and the **Federal Bureau of Investigation (FBI)**, charged 24 defendants, including three licensed clinicians, for Medicare abuse and fraud. Five telemedicine firms, 130 durable medical equipment (DME) companies, and medical professionals concocted a scheme using telemedicine to defraud Medicare upwards of \$1.2 billion.

The involved parties employed a plethora of tactics to trick patients and commit Medicare fraud, the DOJ report reveals. These included:

- » Using international call centers to mine for vulnerable Medicare beneficiaries to sell free or low-cost DME products to.
- » Bribing and giving kickbacks to telemedicine firms to arrange the DME orders.
- » Paying physicians to write up medically unnecessary DME claims after conducting short visits via telemedicine, or even worse, write up claims without speaking with beneficiaries at all.
- » Selling the DME orders garnered from the telemedicine firms to DME companies, who then fraudulently billed Medicare.

"These defendants — who range from corporate executives to medical professionals — allegedly participated in an expansive and sophisticated fraud to exploit telemedicine technology meant for patients otherwise unable to access health care," explains **Brian A. Benczkowski**, DOJ Criminal Division assistant attorney general, in a brief on the case.

DOJ in conjunction with the **Medicare Fraud Strike Force** are taking the lead on these enforcement activities and working closely with officials in New Jersey, the middle district of Florida, and South Carolina as well as the **Internal Revenue Service (IRS)** to settle the case. However, individuals charged in the case reside or practice in other areas of the United States, too, and impact the following states: California, Florida, Missouri, Nebraska, New Jersey, North Carolina, Pennsylvania, South Carolina, Texas, and Washington.

**Note to providers:** The DOJ appears to still be investigating other avenues related to the case. "Any doctors or medical professionals who have been involved with

alleged fraudulent telemedicine and DME marketing schemes — including **Video Doctor USA**, **AffordADoc**, **Web Doctors Plus**, **Integrated Support Plus**, and **First Care MD** — should call to report this conduct to the FBI hotline at 1-800-CALL-FBI,” offers the release.

## Seek Guidance Before You Enter Into a Telehealth Arrangement

Before you embark on a business partnership with a telehealth vendor, you may want to seek legal assistance to determine the logistics of how you’re going to conduct telemedicine at your office. “Telehealth arrangements can be quite complex and require a review by competent healthcare counsel,” advises attorney **John E. Morrone**, a partner at **Frier Levitt Attorneys at Law** in New York City.

“Two critical elements of any telehealth analysis are, (i) does the communication between the physician and the patient comport with applicable state law; and (ii) how is the physician being compensated,” Morrone says.

**Caution:** Not all telehealth and telemedicine companies are the same, as evidenced by the DOJ case. That’s why it’s essential to investigate your business associates before you enter into a contract. “If the physician is not billing the patient or the patient’s insurance the arrangement is likely suspect,” Morrone warns.

“Another red flag occurs if the undue pressure is placed on the physician to approve prescriptions or write orders for other ancillary services,” he adds. “No arrangement should be structured to inappropriately influence the independent clinical judgement of the physician.”

**Tip:** Before you sign on the dotted line with a telehealth company, consider your dealings with your other business

associates like your EHR vendor. “Providers that would like to engage in telehealth need to evaluate the experience of the EHR vendor especially as it relates to their compliance programs. Special attention must be paid to HIPAA and patient privacy issues,” indicates Morrone. “Many vendors inappropriately collect and sell patient data.”

**Resource:** Read all the DOJ details about this billion-dollar case at [www.justice.gov/opa/pr/federal-indictments-and-law-enforcement-actions-one-largest-health-care-fraud-schemes](http://www.justice.gov/opa/pr/federal-indictments-and-law-enforcement-actions-one-largest-health-care-fraud-schemes). □

### Don’t Forget About Malpractice, Too

Being able to assist patients through telemedicine is a wondrous device for providers, but the rules are complicated. Practices must consider things as varied as state liability, procedure, and pharmacy laws as well as medical licensing rules and Medicare Administrative Contractor (MAC) jurisdictions.

**Reasoning:** The majority of telemedicine-related malpractice suits concern medication prescriptions across state lines without a face-to-face visit, explains attorney **Bonnie G. Ackerman**, of the national law firm **Wilson Elser**, in the Professional Liability Advocate blog. “Telemedicine poses unique medical malpractice risks and complicates traditional medical malpractice claims due to distinct issues regarding jurisdiction, procedure and duty of care,” writes Ackerman.

Consider these five liability worries that Ackerman points to before you engage in telemedicine:

1. Liability laws of the state where you practice.
2. State licensing provisions of your state and other states.
3. Statutes of limitations for your state and other states.
4. The intersection of federal and state pharmacy laws and telemedicine.
5. Privacy and security rules and unauthorized medical personnel. □

## Telemedicine

# Master Telemedicine and Telehealth Coding With 3 Key Tips

Plus: Find out why telehealth and telemedicine aren’t the same.

Telemedicine is quickly becoming a relevant form of service by providers in numerous specialties. Whether the physicians in your practice are currently implementing

this clinical method, it’s important that you take into account all that there is to consider when reporting a telemedicine code.

*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 ©2019 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.

**Definitions:** A good place to start is by outlining the difference between telehealth (defined as any health service provided by telecommunications) and telemedicine (defined as any clinical service provided by telecommunications). Additionally, you'll want to consider the array of nuanced guidelines and constantly changing code sets.

Have a look at three key areas to cover some of your most pressing telemedicine and telehealth services' coding needs:

## 1. Keep On Top of Coding Changes in Telemedicine and Telehealth Services

“One of the greatest challenges facing telemedicine coding is that changes in technology typically occur faster than changes in coding,” says **Kent Moore**, senior strategist for physician payment at the **American Academy of Family Physicians**.

“CPT® code change proposals are often generated and acted upon more than a year before the changes/new codes appear in CPT®, and CPT® itself is only published once a year. So, it's easy to see how technology moves faster, leaving coders to wonder if a new telemedicine service fits an existing code or needs to be reported using an unlisted code,” Moore adds.

As an example of this rapid change, the **Centers for Medicare and Medicaid Services (CMS)** introduced two new HCPCS codes for 2019: G2012 (*Brief communication technology-based service, e.g. virtual check-in...*) and G2010 (*Remote evaluation of recorded video and/or images submitted by an established patient...*), which you can use when a provider is evaluating information to determine if a patient needs to be seen in the office.

In addition, CMS added two prolonged service codes, G0513 (*Prolonged preventive service(s) ... first 30 minutes ...*) and G0514 (*... each additional 30 minutes ...*) to the telehealth services' list.

One way to stay current with telemedicine codes is to consult Appendix P in your CPT® manual. Documenting any service listed there when provided via telemedicine is as easy as appending modifier 95 (*Synchronous telemedicine service rendered via a real-time interactive audio and video telecommunications system*). You will also need to add place of service (POS) code 02 (*Telehealth*) to your claim to indicate that the provider is at the distant site (as opposed to the originating site where the patient is located).

**GT no longer needed:** As of January 1, 2018, unless you are billing claims from a critical access hospital (CAH)

under method II for institutional claims, you will no longer need to apply modifier GT (*Via interactive audio and video telecommunication systems*) to a Medicare telehealth claim. But modifier GQ (*Via asynchronous telecommunications system*) is still required for asynchronous communication when appropriate, **Mary I. Falbo, MBA, CPC**, CEO of **Millennium Healthcare Consulting Inc.** in Lansdale, Pennsylvania, reminds coders.

## 2. Understand What Isn't Telemedicine

While telemedicine can involve the use of telephone communication, two groups of telephone evaluation and management (E/M) codes are not regarded as telemedicine.

Codes 99441 through 99443 (*Telephone evaluation and management service by a physician or other qualified healthcare professional ... provided to an established patient, parent, or guardian ...*) and 98966 through 98968

(Continued on next page)

### Feds Finalize Telehealth Expansion for Medicare Advantage

In the past, telehealth was only an option offered through Medicare Advantage beneficiaries' supplemental benefits, but the **Centers for Medicare and Medicaid Services (CMS)** wants to change that.

**Now:** Bolstered by provisions outlined in the Bipartisan Budget Act of 2018 (BBA 2018), CMS updated telehealth services for Medicare Advantage (MA) plans starting in the contract year 2020, notes a two-part final rule, published in the *Federal Register* last month.

“Under this final rule, MA enrollees may have great opportunities to receive healthcare services from places like their homes, rather than being required to go to a healthcare facility,” CMS advises. “MA plans will now have broader flexibility than is currently available in how they pay for coverage of telehealth benefits to meet the needs of their enrollees.”

The final rule allows MA plans the option to offer telehealth benefits to MA patients beyond their supplemental benefits in both rural and urban environments, aligning with BBA 2018 legislation, indicate attorneys **Matthew M. Shatzkes** and **Susan Ingargiola** of the national law firm **Sheppard, Mullin, Richter & Hampton LLP**, in the Sheppard Mullin Healthcare Law Blog.

However, “MA Plans will continue to be able to offer MA supplemental benefits (that is, benefits not covered by fee-for-service Medicare) via remote access technologies and/or telemonitoring for those services that do not meet the requirements for coverage under fee-for-service Medicare or the requirements for MA additional telehealth benefits (such as the requirement of being covered by Medicare Part B when provided in-person),” Shatzkes and Ingargiola explain. □

(Telephone assessment and management service provided by a qualified nonphysician health care professional to an established patient, parent, or guardian ...) are not regarded as telemedicine because CPT® does not regard them as being “face-to-face” services.

The same is true for 99444 (Online evaluation and management service provided by a physician or other qualified healthcare professional ... using the Internet or similar electronic communications network), which is also regarded as non-face-to-face and would also not be defined as telemedicine by virtue of its asynchronous nature.

### 3. Remember That State Laws Differ From Federal Billing Rules

Depending on the nature of the telehealth service and the clinical care administered telemedically, CMS may not cover the outcomes.

“The key to compliance with Medicare rules is to evaluate the Medicare billing requirements for a

bona fide telehealth encounter with the proposed arrangement from the telehealth company,” **John E. Morrone**, a partner at **Frier Levitt Attorneys at Law** in New York City. “It is very common for healthcare services to comport with applicable state law but not be reimbursable by Medicare.”

He adds, “A telehealth encounter may be perfectly acceptable under state law, and even billable to commercial carriers, but not be billable to Medicare.”

**Resource:** For a more in-depth look at CMS’s telehealth services, visit [https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/downloads/Telehealth-Srvcsfctsht.pdf?utm\\_campaign=2a178f351b-EMAIL\\_CAMPAIGN\\_2019\\_04\\_19\\_08\\_59&utm\\_term=0\\_ae00b0e89a-2a178f351b-353229765&utm\\_content=90024810&utm\\_medium=social&utm\\_source=facebook&hss\\_channel=fbp-372451882894317](https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/downloads/Telehealth-Srvcsfctsht.pdf?utm_campaign=2a178f351b-EMAIL_CAMPAIGN_2019_04_19_08_59&utm_term=0_ae00b0e89a-2a178f351b-353229765&utm_content=90024810&utm_medium=social&utm_source=facebook&hss_channel=fbp-372451882894317). □

## HIPAA

# Do CMP Rollbacks Signal Major Changes for HIPAA Enforcement?

Hint: Risk management is even more important now.

After producing record-level HIPAA enforcement numbers last year, the feds shocked many last month with new Civil Monetary Penalty (CMP) guidance. In an about-face turnaround the feds announced that they were drastically reducing penalty caps for HIPAA violations — active immediately.

**Background: The Department of Health and Human Services (HHS)** published the “Notification of Enforcement Discretion Regarding HIPAA Civil Money Penalties” in the *Federal Register* on April 30. Acting on HITECH Act provisions, HHS determined that current CMP caps for HIPAA violations do not differentiate accordingly with the levels of culpability under the four Tiers, indicates the release.

Under the current HIPAA Enforcement Rule, HHS “applies an annual upper limit of \$1.5 million for each of the four culpability Tiers,” reminds the notice. However, that kind of one-fine-fits-all methodology doesn’t seem fair and contributes to the feds’ reasoning. “HHS modified this approach and will now apply a different annual cap to each Tier, thus making the Tiers more meaningful and softening the financial impact of HIPAA violations that

fall into the lower Tiers,” explain attorneys **H. Carol Saul** and **Madison M. Pool** in the Atlanta office of **Arnall Golden Gregory LLP**, in online analysis of the notice.

### Here Are the Details

According to HHS, CMP caps needed to be updated to align with culpability levels outlined in the HITECH Act. In simple terms, it didn’t seem fair that a covered entity (CE) who unknowingly committed a basic HIPAA violation (Tier 1) should have the same annual limit and financial accountability as a CE who willfully neglected to correct actions that led to a HIPAA violation (Tier 4).

“While most of the annual maximums have been reduced, the concept of tying the penalty to the level of culpability has been in the law all along, and the former \$1.5 million annual limit for any type violation didn’t reflect that,” says **Jim Sheldon-Dean**, founder and director of compliance services for **Lewis Creek Systems, LLC** in Charlotte, Vermont. “But keep in mind that the maximums are for any one violation type, and in an incident, there are usually several rules at play, so the maximums can easily be multiplied.”

Take a look at an overview of the CMP cap changes:

| Civil Monetary Penalties for HIPAA Violations |                 |                 |                   |                  |
|-----------------------------------------------|-----------------|-----------------|-------------------|------------------|
| Tier Levels                                   | Minimum Penalty | Maximum Penalty | Past Annual Limit | New Annual Limit |
| 1. No Knowledge                               | \$100           | \$50,000        | \$1,500,000       | \$25,000         |
| 2. Reasonable Cause                           | 1,000           | 50,000          | 1,500,000         | 100,000          |
| 3. Willful Neglect:<br>Corrected              | 10,000          | 50,000          | 1,500,000         | 250,000          |
| 4. Willful Neglect:<br>Not Corrected          | 15,000          | 50,000          | 1,500,000         | 1,500,000        |

\*Information from 45 CFR Part 160, “Notification of Enforcement Discretion Regarding HIPAA Civil Money Penalties,” Tables 1 and 2.

## New Limits May Translate to More Compliance Planning Scrutiny

The reduced limits are sure to come as a relief to providers worried about the financial aftershocks of a breach, but experts warn that practices aren’t off the HIPAA compliance hook. In fact, the changes signal to many that the **HHS Office for Civil Rights (OCR)** is placing more importance on following through on risk management than ever before. And CEs racking up violations must prepare themselves for heightened scrutiny of their compliance planning.

“If an organization does not do a sufficient job of addressing the rules, an incomplete compliance effort, such as ignoring repeated recommendations to reduce risks, can easily be seen as a more culpable situation,” Sheldon-Dean

warns. This puts “the entity into a higher penalty bracket, and the new distinction between penalty levels may provide a greater opportunity for HHS to reasonably use the ‘willful neglect’ levels of penalty.”

That’s why it may be more fiscally savvy to put your money into risk assessment and analysis upfront instead of after the fact.

**Tip:** “The costs of non-compliance are usually far greater than the costs of compliance with HIPAA — the rules are, for the most part, common-sense based,” says Sheldon-Dean. And, he reminds practices not to forget about inflation when calculating annual limits.

“Also, keep in mind that all of the penalty levels have had their numbers adjusted by a roughly 14 percent cost-of-living adjustment, so that the \$1.5 million maximum for a Tier 4 penalty is now \$1,711,533,” explains Sheldon-Dean

**Bottom line:** For the past 13 years, **IBM** and the **Ponemon Institute** have published an annual “Cost of a Data Breach Study,” and as the risks have increased, so have the costs. Last year’s results concluded that “the global average cost of a data breach is up 6.4 percent over the previous year to \$3.86 million,” notes the IBM and Ponemon Institute study. “The average cost for each lost or stolen record containing sensitive and confidential information also increased by 4.8 percent year over year to \$148.” The 2019 report is expected sometime this summer.

**Resource:** Review the “Notification of Enforcement Discretion Regarding HIPAA Civil Money Penalties” at [www.govinfo.gov/content/pkg/FR-2019-04-30/pdf/2019-08530.pdf](http://www.govinfo.gov/content/pkg/FR-2019-04-30/pdf/2019-08530.pdf). □

**\$299.85**

**2019 Physician Coding Bundle**

2019 CPT®, ICD-10-CM  
HCPCS Bundle for Better Reimbursement

**Order Now**

<https://www.codinginstitute.com/pcb2019>

## Reader Questions

### Review This Password Guidance Before Your Next Update

#### Question:

*How often should we change our passwords for our computers? Right now our information technology consultant set it up so we change the passwords every 30 days, but my staff is a bit overwhelmed with the need to constantly remember new passwords, and I think the efforts are distracting them from their jobs.*

Ohio Subscriber

#### Answer:

While frequent password changes have been the norm for years, the **National Institute of Standards and Technology (NIST)** updated their guidelines and recommendations concerning identity security.

“Verifiers **SHOULD NOT** impose other composition rules (e.g., requiring mixtures of different character types or prohibiting consecutively repeated characters) for memorized secrets. Verifiers **SHOULD NOT** require memorized secrets to be changed arbitrarily (e.g., periodically). However, verifiers **SHALL** force a change if there is evidence of compromise of the authenticator,” NIST says (all emphasis original).

With this advice, encourage your IT manager and all your staff who use computers to choose a strong password (or “secret,” in NIST parlance) for each function requiring a password, and don’t require any changes unless you must.

Additionally, NIST does not recommend requiring that passwords have multiple composition rules, like mixed-case letters, numerals, or special characters.

“These rules provide less benefit than might be expected because users tend to use predictable methods for satisfying these requirements when imposed (e.g., appending a ! to a memorized secret when required to use a special character). The frustration they often face may also cause them to focus on minimally satisfying the requirements rather than devising a memorable but complex secret,” NIST says.

When updating your password rules and regulations, NIST recommends creating a “blacklist” of passwords that are common enough to be vulnerable to attack.

To read the rest of the NIST updates, go here: <https://pages.nist.gov/800-63-3/>. □

### What Happened to the HIPAA Audit Program?

#### Question:

*With all the recent news on increased HIPAA enforcement, should we be worried about a federal audit of our privacy controls?*

Supercoder Subscriber

#### Answer:

Though the **HHS Office for Civil Rights (OCR)** Audit Program online resource is still available for review, the HIPAA Phase 2 program isn’t up and running anymore.

“The HIPAA Audit Program has, essentially, been terminated, which is too bad, because the audits, when implemented properly, can be a valuable tool for discovering where there are weaknesses in compliance, either by the fault of covered entities, or through inappropriate regulatory requirements,” says **Jim Sheldon-Dean**, founder and director of compliance services for **Lewis Creek Systems, LLC** in Charlotte, Vermont. “Phase 2 was terminated without coming to a conclusion, and ‘Phase 3,’ yet to come, was identified in the fall of 2018 as a report generating recommendations based on Phases 1 and 2.”

Others agree that the program just seemed to disappear. “Phase 2 of the Audit Program seems to have fizzled out,” laments Philadelphia-based attorney **Edward I. Leeds**, of national law firm **Ballard Spahr LLP**, in online analysis.

Audits may come back down the line, especially since they are tools to help providers overcome compliance issues and manage their HIPAA risks. Leeds advises not to hold your breath. “Although audits may be revived at some time in the future, it is more likely that OCR will dedicate its limited HIPAA resources to investigations,” he writes.

OCR did update 13 questions on its Audit Protocol website last summer, with no major changes to HIPAA. The information was “based on the experience gained in questioning during the 2016 round of audits,” Sheldon-Dean notes. “Despite promises from HHS staff, a change history has not been provided, and the update itself was never announced.”

**Remember:** “Audits are meant to be a learning tool for covered entities and HHS,” reminds Sheldon-Dean. “I

don't think the Audit rules will be used for enforcement purposes, as it would require developing a program, while simply responding to complaints and breaches provides plenty of fruit for making examples of rule violators."

**Tip:** Whether or not the HIPAA Audit Program makes a comeback, there's never been a better time to up your compliance capital with updated policies. Take advantage of this reprieve to assess your risks and act on them with

concrete management tactics. And remember, document everything — because if OCR does roll out the audit patrol, the first thing they'll ask for is written proof of your compliance plan.

Check out the OCR guidance on the HIPAA Audit Program at [www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html#when](http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html#when). □

## Enforcement News

### Public Gets More Time to Comment on Interoperability Rules

Do you need more time to peruse the interoperability rules that the **Centers for Medicare and Medicaid Services (CMS)** and the **HHS Office of the National Coordinator for Health Information Technology (ONC)** released in February? Then you're in for a treat.

**Extension:** HHS decided to extend the deadline to June 3, 2019, giving the public more time to weigh in. "This extension responds to requests from a variety of stakeholders, including healthcare provider organizations and industry representatives," says an HHS release.

Review the nine fact sheets on the ONC rule and submit your comments at <https://www.healthit.gov/topic/laws-regulation-and-policy/notice-proposed-rulemaking-improve-interoperability-health>.

Read the CMS rule in the *Federal Register* and submit your opinion at <https://www.federalregister.gov/documents/2019/03/04/2019-02200/medicare-and-medicaid-programs-patient-protection-and-affordable-care-act-interoperability-and>.

### Hospitals Increasingly Use EHR Data to Improve Care

According to a new report from the **HHS Office of the National Coordinator for Health Information Technology (ONC)**, hospitals are using data garnered from EHR reports to help patients.

**Details:** "As of 2017, 94 percent of hospitals used their EHR data to perform hospital processes that inform clinical practice," indicates the ONC brief. "EHR data is most commonly used by hospitals to support quality improvement (82 percent), monitor patient safety (81 percent), and measure organization performance (77 percent)."

The report looks at a variety of facility types from small, rural clinics to large, urban hospitals, measuring the different ways EHR data is used based on the size and scope of the organization. The data homes in on EHR use between 2015 to 2017.

Take a closer look at the ONC report at [www.healthit.gov/sites/default/files/page/2019-04/AHAEHRUseDataBrief.pdf](http://www.healthit.gov/sites/default/files/page/2019-04/AHAEHRUseDataBrief.pdf).

### Tennessee Company Agrees to Pay \$3 Million to Settle HIPAA Violations

Despite racking up staggering enforcement numbers for 2018, the **HHS Office for Civil Rights (OCR)** 2019 track record seemed to be slowing down, with fewer large-scale breaches on the books. But, a recent big settlement may signal that the feds are ramping up.

**Context:** Franklin, Tennessee-based **Touchstone Medical Imaging** will fork over \$3 million to the OCR and enter into a corrective action plan for dropping the ball on a security incident that exposed 300,000 patients' protected health information (PHI), an OCR release suggests. Touchstone failed to address risks, implement business associate agreements (BAAs), and ignored the loss of ePHI until months after the incident.

"Covered entities must respond to suspected and known security incidents with the seriousness they are due, especially after being notified by two law enforcement agencies of a problem," said OCR director **Roger Severino** in the release. "Neglecting to have a comprehensive, enterprise-wide risk analysis, as illustrated by this case, is a recipe for failure."

See the settlement logistics at [www.hhs.gov/about/news/2019/05/06/tennessee-diagnostic-medical-imaging-services-company-pays-3000000-settle-breach.html](http://www.hhs.gov/about/news/2019/05/06/tennessee-diagnostic-medical-imaging-services-company-pays-3000000-settle-breach.html). □

## 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**

Editor-in-Chief

kristinwh@codinginstitute.com

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

suzanneb@codinginstitute.com

Managing Editor

**Leesa A. Israel, BA, CPC, CUC, CEMC, CPPM, CMBS**

leesai@supercoder.com

Vice President | TCI Content & Online Tools

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 2018 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              | ■ General Surgery             | ■ Ob-Gyn                      | ■ Outpatient Facility     | ■ Practice Management |
| ■ Cardiology              | ■ ICD-10 Coding               | ■ Ophthalmology and Optometry | ■ Part B (Multispecialty) | ■ Primary Care        |
| ■ Emergency Medicine      | ■ Neurology & Pain Management | ■ Orthopedics                 | ■ Pathology/Lab           | ■ Pulmonology         |
| ■ Evaluation & Management | ■ Neurosurgery                | ■ Otolaryngology              | ■ Pediatrics              | ■ Radiology           |
| ■ Gastroenterology        |                               |                               | ■ Podiatry                | ■ 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 - \$399.95
- ☐ Print only - \$299.95
- ☐ Online only - \$199.95

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: P59RAA01



Also Access Your Alert Online at [www.SuperCoder.com](http://www.SuperCoder.com)