Medical Practice Compliance ALERT

News, tools and best practices to assess risk and protect physicians

February 2016 | Vol. 28, Issue 2

Beware false promises from software vendors regarding HIPAA compliance

BY **MARLA DURBEN HIRSCH**

Be careful about relying on assurances of HIPAA compliance and protection from software vendors such as electronic health record (EHR) companies. Those attestations may not be true — leaving you at risk for violations or security breaches you thought you were protected from.

Henry Schein Practice Solutions Inc., the leading provider of office managements software for dental practices, has agreed to pay $250,000 to settle Federal Trade Commission (FTC) charges that it falsely advertised the level of encryption it provided to protect patient data. Schein claimed that its Dentrix G5 software provided industry-standard encryption pursuant to the National Institute of Standards and Technology's (NIST) requirements and ensured that the encrypted software would protect patient data as required by HIPAA.

(SEE **HIPAA**, P. 9)

When claims audit looks bound for DOJ, act first to avoid penalties

BY **ROY EDROSO**

Watch for warning signs that your possible overcoding pattern may get escalated from a Medicare administrative contractor (MAC) to the Department of Justice (DOJ) — and, if it looks like it will, take steps to beat the feds to the punch.

Rhode Island Dermatology and Cosmetic Center and Rhode Island Dermatology in Lincoln, R.I., learned the hard way when they agreed to a $150,000 settlement with the U.S. Attorney in that state. The DOJ's investigation had been based on charges that Rhode Island Dermatology "billed Medicare for surgical closure procedures at a higher rate of complexity than was supported by certain patients' condition or the circumstances of the closure," according to a Nov. 5 press release. The settlement resolved allegations that the practice violated

(SEE **ENFORCEMENT**, P. 2)

IN THIS ISSUE

CONTINUED FROM P. 1

the False Claims Act (FCA), though the practice admits no wrongdoing, according to the U.S. Attorney.

When the feds tune in

MACs and zone program integrity contractors (ZPICs) are usually the first government entities to detect a possibly fraudulent pattern of billing based on their data-mining capabilities. But here are the factors that send a case from the contractors to the Office of Inspector General (OIG) and from the OIG to DOJ:

- **Money.** If a lot of it is involved, that tends to promote cases. One dermatology practice that got nailed for upcoding excisions ended up with a fine of $2.3 million, for example, says Maxine Lewis, president, Medical Coding and Reimbursement, Cincinnati.

But the feds can also get interested just based on the size of the practice's billings, says Glen Prives, an attorney with McElroy, Deutsch, Mulvaney & Carpenter LLP in Morristown, N.J. "Even if charges are legitimate and medically necessary, the highest billers are going to get attention just because [they're] on top of the list, as the government is focused on reining in costs and watching reimbursement."

- **Egregious behavior.** Sometimes contractors are required by law to go to OIG on cases that are "egregious," like billing for unperformed or unnecessary services, says attorney John Morrone, Frier & Levitt, Pine Brook, N.J.
- **Whistleblowers.** Disgruntled employees or patients who rat you out to the government can be cause for federal involvement. The federal government "has done an amazing job of publicizing the benefits of being a whistleblower," says Prives. "It used to be that people in the industry knew about whistleblowers but you didn't see them in the daily paper. Now you do, and as a result, you'll be seeing more of them." Million-dollar payouts on successful *qui tam* prosecutions don't hurt either.
- **Lack of contractor resources.** "Sometimes it's a matter of whether the contractor can easily do the needed level of investigative activity," says Chris Brewer, attorney with Poyner Spruill LLP in Raleigh, N.C. "I had a case that involved incident-to services, and I believe it was referred to OIG because the only way AdvanceMed [the local ZPIC] could be sure about whether or not there was doctor coverage of the mid-levels on any given day of the period was to go to the office, look at the patient ledger and maybe interview the staff." Brewer speculates the ZPIC auditor felt it was more time than he could spare, so he "kicked it upstairs."

Turn yourself in

If law enforcement gets your case, you won't just have administrative recovery with interest to worry about — you'll have to face the possibility of treble damages under FCA, fines, a compulsory corporate integrity agreement and possibly prison. So it helps to beat the feds to the punch.

It would be "highly unusual" to hear about an impending prosecution before you get your subpoena or demand letter, says Brewer. So think fast: If your internal audits pick up a problematic billing pattern, a good first step is to consult with your lawyer and offer to voluntarily report the problem.

To whom should you report? In the event of a simple mistake, go to your MAC; that'll likely be the end of it, says Brewer.

But if it looks deliberate, it's better to self-disclose or go to the U.S. Attorney than to your MAC.

Self-disclosure gives practices a chance to report wrongdoing to the OIG or CMS. "You say: Here's the behavior, here's how we found it out, here's why it happened and why it won't happen again." If you're accepted, you can avoid the treble damages and other noisome features of prosecution, Morrone says.

But self-disclosure is risky. It may be better to negotiate directly with the U.S. Attorney's office in your area. It sounds rash, but Brewer says he's gone with clients and the attorney has said, "We're OK with you taking this to the contractor — thanks for coming in!" Also, while negotiating a settlement technically does not let you off the hook with your contactor, "it's very much the exception that the contractor will take additional administrative action of this type after settlement with DOJ," says Brewer.

Another benefit of this approach is, whether they send you back to the contractor or settle your case, that's probably the end of your *qui tam* worries, says Brewer. "If [whistleblowers] take this same issue to the U.S. Attorney, they're not the first to disclose — you are — so they may be barred from proceeding with a *qui tam* case and getting the money."

RESOURCES:

- DOJ press release: *www.justice.gov/usao-ri/pr/ri-dermatology-and-cosmetic-center-pays-more-150000-settle-allegations-upcoding-medicare*
- DOJ/OIG settlement with Rhode Island Dermatology and Cosmetic Center and Rhode Island Dermatology: *www.justice.gov/usao-ri/file/791061/download*

Telemedicine not immune from fraud and abuse risks

BY **MARLA DURBEN HIRSCH**

Telemedicine is known to come with compliance risks, such as HIPAA privacy and security, scope of practice and medical board licensure issues (*MPCA 5/11/15*). However, one compliance issue previously overlooked when discussing telemedicine can no longer be ignored: fraud and abuse laws.

Telemedicine — also called telehealth — is poised for explosive growth in the United States, from $572 million in 2014 to $2.8 billion in 2022, according to a recent industry analysis.

A large factor of that growth is the move by more payers to reimburse providers for telehealth services. More private payers are encouraging telemedicine as a cheaper alternative to face-to-face office visits, and more than half of the states have enacted "parity" laws, which require insurers to reimburse physicians who provide telemedicine at the same rate as an in-person visit, according to the American Telemedicine Association.

Moreover, federal health care programs are finally beginning to embrace telemedicine. Many states are expanding their Medicaid coverage for telemedicine. Even CMS is easing its restrictions on telemedicine and allowing it in some of its newer payment models — for example, telehealth can be used in place of the face-to-face visit for transitional care management (**99495-99496**). About 50 bills pending in Congress would expand telemedicine use in Medicare further.

This growth is welcome news for many practices, which see the expansion of coverage and reimbursement as a good way to boost revenue. It's also convenient and can improve patient care, says attorney Simone Colgan Dunlap with Quarles & Brady in Phoenix.

However, this expansion of billing and reimbursement for telemedicine services — particularly by publicly funded programs — raises the specter of federal and state fraud and abuse laws, such as kickbacks for referrals and payments above fair market value and will not be immune from such scrutiny, Dunlap says.

The Office of Inspector General (OIG) also has gone on record that while it encourages technological advances, it will not allow new technology to mask unlawful arrangements, warns attorney Scott Grubman, former U.S. assistant attorney who is now with Chilivis, Cochran, Larkins & Bever LLP, Atlanta.

While some activities are obviously troublesome, such as improper billing, some of the fraud and abuse issues that can arise with telemedicine aren't necessarily apparent, perhaps since they're being applied to a newer concept.

"It's still uncharted territory," says attorney Ed Rickert with Quarles & Brady in Chicago. For instance, even if Medicare doesn't reimburse for telemedicine in a particular instance, if the providers involved are in a position to refer other services reimbursable by Medicare to each other, the anti-kickback and/or Stark laws can still be implicated.

So if you're delving into telemedicine, take these three steps:

1. **Incorporate your fraud and abuse analysis into these services.** Carefully consider whether a telemedicine deal might possibly implicate the fraud and abuse laws and structure the arrangement so that it passes muster. It's best if you can fit the deal into a Stark exception or anti-kickback safe harbor, adds Rickert.

2. **Include telemedicine services as part of a practice's overall compliance program.** "There's so much more scrutiny now, especially with the False Claims Act and [whistleblowers]," warns Dunlap.

3. **Watch for state laws.** For instance, make sure that a telemedicine consulting deal between a specialist and primary care physician doesn't run afoul of state fee-splitting prohibitions. Private payers also may rely on state fraud and abuse laws to challenge problematic activities.

RESOURCE:

- Telemedicine industry analysis: *www.grandviewresearch.com/industry-analysis/us-telehealth-market*

CFAA may extend practice's reach after HIPAA breach

BY **MARLA DURBEN HIRSCH**

Because HIPAA doesn't provide a private right of action, practices can't use the law to sue hackers or rogue employees who access electronic patient data. However, practices may have more ammunition to fight back: suing the perpetrator of the access or misuse for violating the Computer Fraud and Abuse Act (CFAA).

The CFAA is a federal law that prohibits fraudulent access to "protected" computer information. The purpose is to prevent access that is unauthorized or that exceeds the user's authority to information not in the public domain, such as patient data or trade secrets, says attorney Lucy Li with Fox Rothschild in San Francisco. In addition to criminal prosecution, the CFAA allows the victim to file a civil lawsuit for injunctive relief and to recover losses, such as the cost of investigating the event, damage to the computer system or nonphysical damage, such as economic loss. "It's one tool to help you get compensated," Li notes.

Applicability varies by state

The CFAA, sometimes known as the "federal anti-hacking law," always applies to outside hackers, says attorney Paul Freehling with Seyfarth Shaw in Chicago.

Interestingly, it also applies in many states when a former employee accesses the practice's computers after he's been fired but before the practice locked him out of the system, or when an employee with limited access views and uses records that she's not authorized to access. This means that employers have more power than simply disciplinary action against the employee.

However, the reach of the CFAA to employees, former employees and contractors who have access to the employer's computers depends on the state where the access occurred and the circumstances surrounding the authorization for access. In most states, the misuse of the information is a violation of the CFAA regardless of the authorized status of the employee, says Freehling.

A few federal circuit courts take a narrower view of the definition of "exceeds authorized access," holding that as long as the employee was permitted to be on the employer's computer for any purpose, diversion of employer information is not a violation of the CFAA. In other words, the act prohibits unlawful access to a computer but not unauthorized use of the electronic information.

For instance, a California district court recently ruled that a laboratory provider, Loop AI Labs, could not use the CFAA to sue its former Chief Executive Officer Anna Gatti for misappropriating trade secrets and attempting to frustrate the success of the company in order to force its sale. Although she had left the company and worked for a competitor, Loop AI Labs had not yet blocked her access to its computers, and she was able to log in and obtain the information. The court ruled that until Loop formally revoked her authorization to access the computers, she didn't violate the CFAA by logging in, notes Freehling. Her motive wasn't relevant.

4 CFAA tips for practices

The CFAA is a limited yet handy way to recover money from a bad actor who causes a HIPAA breach or otherwise misappropriates private electronic information. To reduce your risk of unauthorized access and to improve your chances of using the CFAA should you be a victim, take these four steps:

1. **Protect your data.** Make sure your firewalls and security patches are up to date and your employees are using passwords. "Prevention is best. Litigation to recover is costly," says Li.
2. **Limit and monitor electronic access.** Be careful who you give access to to begin with. Don't allow more authority than is necessary for employees to perform their job duties, says Li. Keep what is "authorized" access as narrow as possible.
3. **Disable login credentials immediately** when an employee resigns or is terminated. This is particularly important if you're in a state, such as California, that ascribes to the more narrow view of the CFAA, says Freehling.
4. **Don't forget state law.** You may be able to bring state causes of action, such as trade secret appropriation for stealing patient lists or state computer fraud laws. Those laws may be particularly helpful in jurisdictions or situations where the CFAA doesn't apply.

RESOURCE:

- Loop AI Labs v. Gatti decision: *www.tradesecretslaw.com/files/2015/09/Order-Motion-to-Dismiss.pdf*

Heed new meaningful use exception deadline; CMS eases the filing process

BY **RICHARD SCOTT** AND **JULIA KYLES, CPC**

Physician groups will be eligible to apply for an exception for multiple eligible professionals (EPs) through a single application, according to an updated hardship-exception protocol released Jan. 22. Previously, all providers had to file an individual exception, even those in the same practice.

That will make it easier for practices to avoid a 3% pay cut in 2017.

"This is very welcome news," says Rob Tennant, senior policy adviser for the Medical Group Management Association (MGMA) in Washington, D.C., who says providers will see a "significantly streamlined hardship application process" as a result of the program changes.

This is very welcome news.

ROB TENNANT, SENIOR POLICY ADVISER, MGMA, WASHINGTON, D.C.

Deadline gets pushed up

Forget the July 1 deadline. The new filing deadline is March 15, and the reasons an EP can cite for filing a hardship remain the same.

Another reprieve is a shortened application form, which should make filing less onerous than in years past. Providers that choose to submit with multiple EPs on a single application will need to provide all national provider identifiers (NPIs) on the form, notes CMS.

Remember that certain specialties — including anesthesiology, diagnostic radiology, interventional medicine, nuclear medicine and pathology — are automatically excluded. Be sure to follow best practices when submitting your application, such as submitting by email and storing a receipt.

The relaxed filing process arrives after Congress directed CMS to simplify meaningful use exceptions through the Patient Access and Medicare Protection Act (PAMPA), which introduced the review of "categories" of EPs (*see story, p. 6*).

Don't miss the penalty appeal deadline

EPs that will receive the meaningful use penalty based on their 2014 performance have an earlier deadline. They must submit the appropriate payment adjustment reconsideration application — for single EPs or multiple EPs — together with any supporting documentation by Feb. 29.

"Only apply if you received a letter from Medicare indicating that you are subject to the 2016 payment adjustment," CMS says on the electronic health record (EHR) incentive website. In the application instructions, CMS notes the process is for EPs that feel the penalty assessment was applied in error. The agency strongly encourages EPs to submit the application via email but provides a fax number to be used as a final resort.

RESOURCE:

- Filing instructions and applications: *www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/HardshipInstructions.pdf*

PAMPA eases EHR hardship exceptions, has 3 more compliance changes

BY **MARLA DURBEN HIRSCH**

Don't miss the good news in the Patient Access and Medicare Protection Act signed Dec. 29 by President Barack Obama. The new law does more doesn't just tweak several payment rules under the Medicare program; it contains four provisions that affect compliance, including an easier road to a meaningful use exception:

1. New hardship exception under the electronic health record (EHR) meaningful use program. The law adds flexibility for eligible professionals and eligible hospitals that may not be able to comply with the program's reporting requirements for 2015. The new exception allows CMS to exempt "categories" of providers, not just applications on a case-by-case basis, as was previously provided. Those who meet the exception will avoid Medicare payment adjustments in 2017. CMS announced Jan. 22 that it has streamlined its forms and will allow groups of providers to apply for an exception on one application but is not creating new hardship exception categories. The deadline for eligible professionals to apply for this new exception is March 15; for hospitals the deadline is April 1. *See story, p. 5 for more information on the hardship exception.*

2. More data sharing between Medicare and Medicaid programs. The law improves the sharing of data in the Medicare-Medicaid Data Match as part of the ongoing attempt to improve program integrity and oversight. The change will make it easier to detect and stop improper payments to providers who treat dual-eligible patients — patients who are covered by Medicare and Medicaid.

3. Medicare administrative contractors (MACs) incentivized to reduce payment errors. Expect MACs to ramp up pre- and post-payment medical review and to institute stricter local coverage determination policies before Medicare institutes incentives and payment adjustments designed to reduce MAC payment error rates. The change won't kick in for at least three years, but don't assume MACs will wait to act. The incentives and adjustments may include sliding scales of awards or reductions based on error rates and/or on accomplishing certain tasks.

4. New penalties for ID theft. The law strengthens the penalties for the illegal distribution of a provider's Medicare, Medicaid or CHIP identification number or unique health identifier. The law increases the penalty for the unauthorized purchase, distribution or sale of such an identifier to no more than 10 years in prison and/or a fine of no more than $500,000 ($1 million for corporations).

RESOURCES:

- Patient Access and Medicare Protection Act: *https://www.congress.gov/bill/114th-congress/senate-bill/2425/text*
- CMS hardship exception website: *https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/paymentadj_hardship.html*

Subscriber information

EDITORIAL
Have questions on a story? Call or email:

Content Manager, Medical Practice:
Karen Long, 1-301-287-2331
klong@decisionhealth.com

Editor:
Marla Durben Hirsch, 1-301-287-2700
mhirsch@decisionhealth.com

SUBSCRIPTIONS
Direct questions about newsletter delivery and account status, toll-free, to 1-855-CALL-DH1 or email to: *customer@decisionhealth.com*.

COMPLIANCE LISTSERV
To join our free Internet forum on fraud and abuse issues, go to *http://listserv.ucg.com/cgi-bin/listserv/listserv.pl/fraud-l*, click on the "Join the Fraud & Abuse Discussion Group" link, and follow the instructions.

COPYRIGHT WARNING
Copyright violations will be prosecuted. *Medical Practice Compliance Alert* shares 10% of the net proceeds of settlements or jury awards with individuals who provide essential evidence of illegal photocopying or electronic redistribution. To report violations contact: Steve McVearry at 1-301-287-2266 or email *smcvearry@ucg.com*.

REPRINTS
To request permission to make photocopy reprints of *Medical Practice Compliance Alert* articles, call 1-855-CALL-DH1 or email customer service at *customer@decisionhealth.com*. Also ask about our copyright waiver, multiple copy and site license programs by calling the same number.

Medical Practice Compliance Alert® is a registered trademark of DecisionHealth. DecisionHealth is a registered trademark of UCG. *Medical Practice Compliance Alert* is published 24 times/year by DecisionHealth, 9737 Washingtonian Blvd., Ste. 200, Gaithersburg, MD 20878-7364. ISSN 1047-1863. *www.decisionhealth.com* Price: $547/year.

Copyright © 2016 UCG DecisionHealth, all rights reserved. Electronic or print redistribution without prior written permission of DecisionHealth is strictly prohibited by federal copyright law.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered and is NOT intended to be used as a substitute for legal advice. It is published 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 service of a competent professional should be sought.

7 steps to prepare for, handle new fraud focus on doctors

BY **MARLA DURBEN HIRSCH**

For physicians, it's time to take compliance more seriously, now that the government has clearly stated that doctor are in the enforcement limelight (*MPCA 1/16*). Physicians should take these seven tips:

1. Rev up that compliance program. "If you're not doing compliance because of the cost and you get investigated, you're being penny-wise and pound-foolish. The cost of a compliance program is nothing compared to the cost of an investigation, especially with individual accountability. Don't think it won't happen to you," warns Mary Cummings, adjust professor and director, Health Care Compliance Online with the University of Pittsburgh School of Law.

2. Review all of your business arrangements from a compliance standpoint. "Make sure you're in compliance. If you have an arrangement, don't assume the other side has vetted it. And you can't take comfort that the DOJ [Department of Justice] won't care about small fish" because that's no longer the case, says attorney Scott Grubman, former U.S. assistant attorney who is now with Chilivis, Cochran, Larkins & Bever LLP, Atlanta.

3. Pay attention to your relationships with manufacturers. See whether those deals are worth having, and if so, whether they're structured in a lawful manner, says attorney Alyce Katayama with Quarles & Brady in Milwaukee. Those arrangements are not only high on the government's enforcement radar because of the high incidence of kickbacks, they're also publicly available as part of CMS' Open Payments program.

4. Review the requirements of "Upjohn warnings" and the difference between counsel for the practice versus counsel for the people working for it, says attorney Brian Flood with Husch Blackwell in Austin, Texas. Employees are entitled to know their rights and the company's role. "There's a duty to defend versus a duty to disclose," says Flood, who recommends that this be added to a practice's compliance programs. If you're not familiar with Upjohn warnings, confer with an experienced health care fraud attorney to determine when and how they apply.

5. Be careful when accepting help from sales representatives and others in filling out prior authorization forms. Assistance for prior authorization is becoming more common, but it's unresolved whether such assistance is itself a kickback even if the justification for the authorization is real, warns Katayama. However, some assistance activities, such as the use of canned language and falsifying forms are clearly not acceptable, as demonstrated in the Warner Chilcott guilty plea and settlement and the indictment of Dr. Rita Luthra for, among other things, allowing this to occur. "In Luthra's case, her staff didn't lift a finger. The sales reps were accessing her electronic health records and writing prior authorizations pretending to be a doctor. That's really stupid," Katayama notes.

6. Review your insurance policies to see whether they address and/or cover both individual accountability and liability for reporting an individual to the government, says Flood.

7. Don't forget about HIPAA. While the DOJ is focused on fighting fraud, waste and abuse, it won't shy away from enforcing HIPAA when it happens to also uncover a HIPAA violation, as it did against Luthra, who allowed pharmaceutical sales reps to access her patients' records without patient authorization. Luthra has now been criminally charged for violating both the anti-kickback statute and HIPAA.

RESOURCES:

- Warner Chilcott settlement
  www.justice.gov/opa/pr/warner-chilcott-agrees-plead-guilty-felony-health-care-fraud-scheme-and-pay-125-million
- Indictment of Rita Luthra, M.D.
  www.justice.gov/usao-ma/pr/springfield-doctor-indicted-anti-kickback-case

3 drug screen FAQs to protect labs from improper payments

BY **JULIA KYLES, CPC**

Abusive and fraudulent drug screen billing is on the radar of investigators and CMS. As part of its effort to stop improper payments for the service, CMS this year released a completely new set of drug screen codes that private payers have started to adopt.

To make sure your lab isn't attracting the attention of auditors, investigators and prosecutors, share these three reader-submitted questions with your lab, coding and compliance staff:

Question: *I'm trying to understand the difference between* ***G0477*** *and* ***G0478.*** *Does the term presumptive in G0477 mean that we presume we will find the medication we've prescribed and use G0478 for other substances?*

Answer: Both codes are presumptive. According to the CPT manual, presumptive tests are done to identify use or non-use of a drug. However, when a presumptive test is positive for a drug class, it doesn't provide details. Positive results for a presumptive test may justify more detailed definitive testing. For example, when a presumptive test is positive for amphetamine, the provider might order a definitive test to determine whether the patient was taking allergy medicine or an illicit form of the drug.

The difference between the two codes is how you perform the test and read the results.

Use G0477 when the result is read by direct optical observation only, such as when the dipstick is inserted in the sample and a line appears on the dipstick.

Use G0478 when the result is read by "instrument-assisted direct optical observation," such as when the technician inserts with a dipstick with a sample into the device and the results appear on a screen.

Labs that have a CLIA certificate of waiver should take extra care when working with the new code set.

Labs that have a Clinical Laboratory Improvement Act (CLIA) certificate of waiver should take extra care when working with the new code set. Billing for a more complex — and higher-paying — code could look like an attempt to game the system.

Question: *Our normal protocol is to run a simple presumptive drug screen on patients (the results are read on the cup). Because the results for the simple tests often have false negatives, we confirm the results with a second presumptive screen on our chemistry analyzer. How do we report that with the new codes?*

Answer**:** You cannot report two presumptive drug screens for the same patient and the same day. The simple test would be reported with G0477. The chemistry analyzer test would be reported with **G0479** (Drug tests[s], presumptive, any number of drug classes; any number of devices or procedures by instrumented chemistry analyzers [e.g., immunoassay, enzyme assay, TOF, MALDI, LDTD, DESI, DART, GHPC, GC mass spectrometry], includes sample validation when performed, per date of service).

Note that sample validation is included in all of the new tests.

Question: *I have billed several insurers for an instant drug screen with G0477 and modifier* ***QW.*** *All of the claims have been denied. Is the QW modifier causing the denial, and if so, does that mean we don't need a CLIA certificate to report the test?*

Answer: Check your remittance advice to see if the modifier is causing the denial. Medicare's clinical lab fee schedule did not list modifier QW (Clinical Laboratory Improvement Act- [CLIA] waived test) with the code.

However, labs must maintain the appropriate CLIA certificate in order to bill for lab services

CONTINUED FROM P. 1

However, Schein continued to market the software as secure and HIPAA compliant after the software developer informed Schein that the software used a less complex method of data masking not up to NIST standards, making it less secure. In addition, NIST had published a vulnerability alert. Instead, Schein rebranded it as "data camouflage" or data masking rather than encryption, says attorney Elizabeth Litten with Fox Rothschild in Princeton, N.J. By the time that Schein announced that the product wasn't up to snuff, it was too late to avoid the FTC enforcement action.

In addition to the $250,000 settlement for making the false and misleading claims, Schein is barred from misleading customers about the extent of the encryption its software provides and is required to notify its customers that the product doesn't provide industry-standard encryption.

Impact on practices is unknown

It is unclear how much damage Schein's false and misleading statements have caused dental practices and patients since it's still unknown whether the lack of encryption caused any practice to suffer a breach. However, the practices Schein duped into believing that their data was protected by encryption and in compliance with HIPAA may have skimped on other safeguards as a result, leaving the records vulnerable, warns attorney Michael Kline also with Fox Rothschild. "The encryption safe harbor [in the event of a breach] would not apply, and practices may not have included this in [their] risk analyses," he points out.

Not only are practices now more vulnerable than they thought, but they need to reassess their risks, determine whether a breach of unsecured information occurred and if so, retroactively report to patients, HHS and the media, warns Litten.

Practices also may have a related problem. If the dentists relied on Schein's assurances that the data was encrypted and used that to advertise or market the practice to patients, the practices could be found liable by the FTC for misleading or deceptive trade practices, warns Kline.

"You can't hide behind the foibles of a company you retained to help you comply with HIPAA," he warns.

FTC enforcement can be triggered even if no data breach occurs. There was no allegation that a beach occurred with Schein's software; it was the false and misleading statements that tripped the company up, says Litten.

"I'm sure there will be lawsuits on this. It's wild and wooly out there, and you don't know the quality of the wool you're buying," says Kline.

Use 6 tips to reduce your risk

This type of problem is going to increase as more physicians and health care professionals adopt EHR systems, practice management systems, patient portals and other health IT, says Litten. To protect your practice, take these six steps:

1. Vet the software vendor regarding the statements it's making to secure and protect your data. If the vendor is claiming to provide NIST-standard encryption, ask for proof. See what it's saying in its marketing brochures. Check references, Google the company for lawsuits or other bad press, and ask whether it suffered a security breach and if so, how the vendor responded.

2. Make sure that you have a valid business associate agreement that protects your interests when the software vendor is a business associate, says Kline. For instance, a vendor that merely provides you with software but doesn't store or handle your data may not be a business associate, but a vendor that accesses your data to provide maintenance or training or a cloud vendor that stores the data and is more than a conduit can be a business associate.

3. Check whether your cyberinsurance covers this type of contingency. It's possible that it doesn't cover misrepresentations, and you should know where you stand, warns Litten.

4. See what protections a software vendor contract may provide you. For instance, if a problem occurs with the software or it's not as advertised, is the vendor obligated to provide you with an upgrade, a refund, termination of the contract and/or damages? If not, you might want to add such protections, using the Schein settlement as leverage.

5. Don't market or advertise that you provide a level of HIPAA protection or compliance on your website, Notice of Privacy Practices or elsewhere unless you're absolutely sure that you do so. Don't forget that the FTC has been making inroads in patient privacy and security and has taken an aggressive stance against violators. "The FTC is greatly increasing its enforcement activity," Kline says.

6. Look at your legal options if you find yourself defrauded. For instance, the dentists who purchased the software under false pretenses have grounds for legal action, says Kline.

RESOURCE:

- FTC announcement of Henry Schein settlement: *https://www.ftc.gov/news-events/press-releases/2016/01/dental-practice-software-provider-settles-ftc-charges-it-misled*

Expect specialty, POS to factor in prolonged services audits

Prolonged services snapshot

- Outpatient reporting rose 185% for podiatry.
- Clinical nurse specialists' use of inpatient prolonged services increased by 303%
- Reporting by internal medicine specialists is down an average of 14%

A review of prolonged services is on the to-do list of federal auditors, and *MPCA's* review of Medicare's claims data indicates that certain providers are more likely to receive scrutiny.

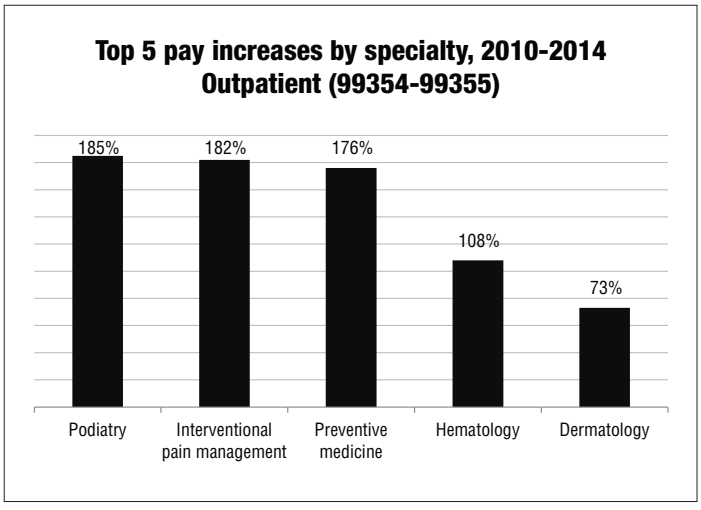
The HHS Office of Inspector General (OIG) will check claims for prolonged services to make sure the time-based services and the payments, which start at $92 for one unit of service, met Medicare's requirements.

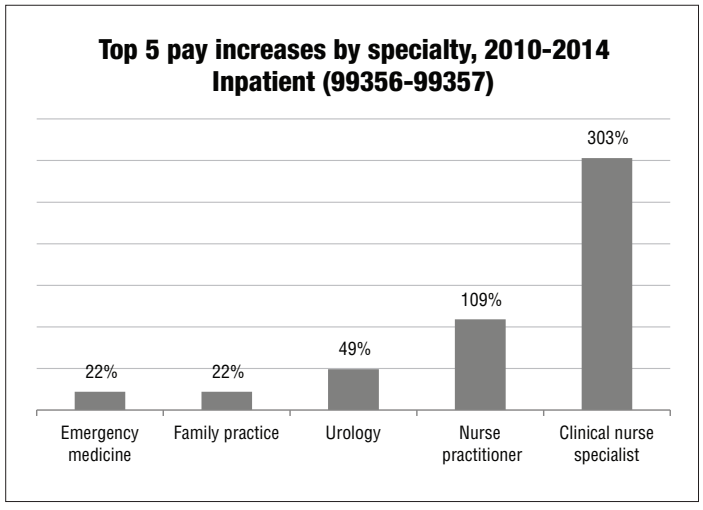
The agency didn't specify whether it will review office and outpatient services (**99354-99355**) or inpatient services (**99356-99357**). However, the OIG did note that the services should be rare and unusual *(MPCA 11/23/15)*.

Based on an analysis of claims data for 2010-2014, some specialties' use of the codes has exploded. Providers in specialties that have had rapid utilization and payment increases could receive auditor attention before specialties where utilization is high but stable. For example, family practice received more than $34 million for in-office prolonged services during the four-year period, the second-highest amount for all specialties. However, its utilization increased by a mere 8%.

Prolonged services payments to internal medicine providers topped the list for all specialties. They earned more than $100 million for outpatient and inpatient services combined, according to the latest data. But that represents a decrease in payments. They received 15% less for outpatient services and their payments for inpatient services fell 13% during the same period.

These numbers provide a basic guide for auditors to determine what's unusual. The following charts show the specialties that are likely to attract an auditor's attention based on where the services were performed. The specialties had the largest increases in utilization combined with high earnings. In 2014 — the latest available data — the total payments to the featured specialties averaged $113,022 for outpatient services and $741,033 for inpatient services.





Copyright Notice

How did you get this email?

It is illegal to forward this electronic version of ***Medical Practice Compliance Alert*** to anyone else. It is a free benefit only for the individual listed by name as the subscriber. It's illegal to distribute electronically ***Medical Practice Compliance Alert*** to others in your office or other sites affiliated with your organization. If this email has been forwarded to you and you're not the named subscriber, that is a violation of federal copyright law. However, only the party that forwards a copyrighted email is at risk, not you.

To confidentially report suspected copyright violations, call our copyright attorney Steve McVearry at 1-301-287-2266 or email him at *smcvearry@ucg.com*. Copyright violations will be prosecuted. And ***Medical Practice Compliance Alert*** shares 10% of the net proceeds of settlements or jury awards with individuals who provide essential evidence of illegal electronic forwarding of ***Medical Practice Compliance Alert*** or photocopying of our newsletter.