30 Years HCCA

Report on
PATIENT PRIVACY

Volume 26, Number 11 • November 2026

Practical News and Strategies for Complying With HIPAA

Contents

Page 3
Patient Privacy Court Case

Page 5
ONC 'Unleashing Prosperity' Rule Keeps Privacy, Security Certification Criteria

Page 6
OCR's Noonan Shares SUD Complaint, Breach Data, No Guesses on Privacy Reg

Page 8
Multistate Labcorp Settlement Called 'Roadmap' for CEs to Manage Vendors

Page 10
TEFCA Disruption After Update Prompts Broad Complaint from Consumer Group

Page 11
Privacy Briefs

Editor
Theresa Defino
theresa.defino@hcca-info.org

Writer
Jane Anderson

Copy Editor
Julia Ramirez Burke
julia.ramirez.burke@hcca-info.org

Access Complaint By Lawyer Triggered $140K OCR Deal With Dentist; $11M Award Is Unpaid

More than six years ago, Pennsylvania attorney Braden Lepisto fired off an access complaint to the HHS Office for Civil Rights (OCR) because he couldn't get his client's dentist to provide her medical records.

Lepisto was trying to prove that Mary Heffelfinger had developed tongue cancer and was permanently disfigured due to the negligence of her dentist, Linda Shen. Heffelfinger was ultimately awarded $11.5 million following a February 2024 jury trial, an amount that included $8 million in punitive damages, in part because of the same records issue. Lepisto's malpractice judgment was upheld by the Pennsylvania Supreme Court in July 2025 (and another appeal was denied earlier this year). Yet, he has been unable to collect more than a "minuscule" amount from Shen.

The OCR investigator handling Lepisto's access complaint "periodically would contact me and ask for information, ask for the status of the case and whether we had received the records. At some point, she didn't ask for more information, and each time that I asked for an update, I was essentially told, 'I can't tell you anything,'" Lepisto, a partner with Kline & Specter PC, exclusively told *RPP*. "I think my last interaction with the investigator from OCR was around 2022."

Was OCR's Approach the Right One?

So Lepisto "had no idea" that OCR had reached a settlement with Shen, resolving the agency's investigation triggered by his complaint, until *RPP* contacted him on Oct. 29. That was three weeks after OCR announced Shen agreed to pay OCR $140,000 to settle allegations that she violated two HIPAA provisions—lack of safeguards and policies and procedures.[1]

This case is arguably the most disturbing in OCR's coterie of 55 previous access enforcement actions, a number already so high that such settlements—which generally cite tardy or costly records access—may garner little more than a glance. Yet Shen's settlement begs the question of whether OCR took the right approach with her.

OCR said it gave her a 90% break on the penalty because she is a solo provider and the agency didn't want to put her out of business. The settlement also doesn't require her to follow a corrective action plan (CAP) or take any steps to improve her practice, despite the litany of chaotic conditions OCR itself documented.

Neither Shen nor her attorney, Andrew J. Katsock III, responded to *RPP*'s repeated requests for comment. Katsock represented Shen in the malpractice case; he also signed the settlement agreement on her behalf.

News of the settlement both surprised and disappointed Lepisto. "I am glad that HHS and OCR followed through with their investigation and did something. However, I am disappointed in the result," he said.

Settlement 'Hurts' Patient at Its Center

"I don't know if [OCR officials] knew the extent of her conduct and the harm that it caused," Lepisto said, adding that without a CAP, Shen "can continue on in the way that she'd practiced before." He would have preferred Shen either pay no fine or that at least some of it was given to his client—which likely would have happened if OCR had done its job writing such a regulation more than 10 years ago.

The $140,000 "should be going towards paying off the judgment. That's why seeing this was disappointing, because there was no communication with the ultimate victim of this—Mary. And it just ended up in this apparent settlement that is now actually hurting my client," Lepisto said.

"Mary deserves payment for the injuries that she suffered and for the judgment that she received," he said, adding that he has had to hire a law firm to try and collect on the $11.5 million because "Shen has not in any way tried to cooperate or showed any willingness to pay off the judgment that is owed."

He said the attempts to recover funds showed Shen had no ability to make a large payment like she made to OCR, adding yet another surprise to Lepisto's list.

Neither Heffelfinger nor Lepisto are identified in the documents OCR shared, but *RPP* made the connection to Shen. Lepisto confirmed to *RPP* that he is the "attorney for a former patient" mentioned in the settlement who sent OCR the access complaint on April 21, 2020.

OCR: Access Denial Wasn't a Violation

Records *RPP* reviewed show Shen has been dogged by complaints of mishandling records for years. But nowhere do OCR's documents mention the malpractice case, even though both hinged on the inappropriate handling of records, or the fact that Shen was disciplined and her license temporarily suspended by the state for similar issues while OCR's investigation was ongoing.

Ironically, OCR determined it could not cite her for failing to produce the records because she claimed she didn't have them. "Because the right of access under the Privacy Rule requires the production of PHI [protected health information] as long as it is maintained in the designated record set, OCR did not pursue an access violation against Shen Smiles," according to its July 31, 2024, notice of proposed determination.[2]

Report on Patient Privacy (ISSN: 1539-6487) is published 12 times a year by Health Care Compliance Association, 6462 City West Parkway, Eden Prairie, MN 55344. 888.580.8373, hcca-info.org.

Copyright © 2026 by the Society of Corporate Compliance and Ethics & Health Care Compliance Association. All rights reserved. On an occasional basis, it is okay to copy, fax or email an article from *RPP*. Unless you have HCCA's permission, it violates federal law to make copies of, fax or email an entire issue; share your subscriber password; or post newsletter content on any website or network. To obtain permission to transmit, make copies or post stories from *RPP* at no charge, please contact customer service at 888.580.8373 or helpteam@hcca-info.org. Contact Paule Hocker at paule.hocker@corporatecompliance.org or 888.580.8373 if you'd like to review our reasonable rates for bulk or site licenses that will permit redistributions of entire issues.

Report on Patient Privacy 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 services of a competent professional person should be sought.

Subscriptions to *RPP* include free electronic delivery in addition to the print copy.

To order an annual subscription to **Report on Patient Privacy** ($499 for HCCA members; $679 for nonmembers), call 888.580.8373 (major credit cards accepted) or order online at hcca-info.org.

Subscribers to this newsletter can receive 12 non-live Continuing Education Units (CEUs) per year toward certification by the Compliance Certification Board (CCB)®. Contact CCB at 888.580.8373.

$11.5M Awarded Two Years Before OCR Settled

Moreover, that document states that OCR's "investigation did not uncover evidence that Shen Smiles' failure to implement policies and procedures and to safeguard PHI resulted in physical harm, financial harm, reputational harm, nor that it hindered an individual's ability to obtain healthcare."

Yet that claim is directly contradicted by the facts resulting in the $11.5 million judgment, which the jury awarded after a three-day trial five months *before* the letter was written. The Supreme Court ruling upholding the award occurred more than a year before OCR settled with Shen.

The disorder OCR did find was clearly outlined in the notice of proposed determination, which quotes from a letter OCR sent to Shen in November 2023 at the conclusion of its inquiry. After he reviewed this document, Lepisto told *RPP* he found the same conditions, and worse.

"OCR's investigation determined that Shen Smiles does not reasonably safeguard PHI from any intentional or unintentional use or disclosure of PHI that would violate the requirements of the Privacy Rule, as required by 45 C.F.R. § 164.530(c)," the agency told her.

OCR's documents don't even hint at the epic—and unsuccessful battle—Heffelfinger and Lepisto waged to get the records nor the stage IV cancer diagnosis and multimillion malpractice judgment.

Dentist Answered 'None' When Asked for Policies

OCR said it "learned during its investigation that:

- "Patient records are not maintained in order and are not in locked file cabinets or otherwise physically safeguarded. Patient records are stored in unsecure locations including in clear plastic boxes in the hygienist's office, on the floor, and in boxes in a private bathroom.
- "Records are carried from one practice location to the other and to Dr. Shen's home and are regularly missing when patients arrive for appointments.
- "Dr. Shen believed that a former office manager illegally took records from the practice, including Affected Party's records. Dr. Shen stated that she did not reprimand or discipline the employee or take other action to stop the behavior.
- "Shen Smiles did not provide its employees any formal HIPAA Privacy Rule training."

The agency also described its own experiences with Shen, writing in the letter of opportunity that she objected to OCR's data requests and never sent required documents, even for evidence of "newly reported illegal removal of patient records from Shen Smiles' office."

OCR noted that, "on April 25, 2021, Shen Smiles responded to OCR's February 24, 2021, data request. In

continued on p. 4

EDITORIAL ADVISORY BOARD: ***JEFFREY DRUMMOND,*** Esq., Partner, Jackson Walker LLP, Dallas; ***ADAM H. GREENE,*** Esq., Partner, Davis Wright Tremaine LLP, Washington, D.C; ***REECE HIRSCH***, Esq., Morgan, Lewis and Bockius LLP, San Francisco; ***KIRK J. NAHRA,*** Esq., Partner, WilmerHale, Washington, D.C.

PATIENT PRIVACY COURT CASE

This column is designed to highlight legal actions taken by state, federal and other oversight authorities and explores the court challenges and regulatory risks facing HIPAA covered entities and business associates.

◆ **In 2024, despite having more than 300 doctors who practiced in 60 locations in New York and five in Connecticut, Boston Children's Health Physicians (BCHP) had just two employees who were "responsible for overseeing the company's IT and information security functions." Instead, BCHP relied on two IT vendors—one handled "both management of and security for BCHP's company's active patient records system," while the second was contracted "for the management of (not security for) BCHP's other IT systems."**

The reason this setup is known is because BCHP experienced a breach in August 2024 via its IT vendor and business associate, Axispoint Technology Solutions Group Inc., now known as XTIUM after it merged with Evolve IP and changed its name. According to its website, "XTIUM is an AI-Native managed services provider."

To resolve allegations of violations of the Security Rule and two state laws, the organizations jointly recently settled with the attorneys general (AGs) of New York and Connecticut for $2.7 million, but the agreement doesn't say how that amount is being split between the two firms. Neither BCHP nor XTIUM admitted wrongdoing.[1]

Under the settlement, announced Oct. 16, BCHP could be required to pay the states an additional $1.3 million if it breaches the agreement at any time in the next 10 years.[2] New York would receive $1,040,000 and $260,000 would go to Connecticut. It is not clear why BCHP alone is facing an additional fine.

For now, the $1.3 million is suspended, and both organizations agreed to implement a number of security upgrades and enhancements. The 26-page settlement is worthy of review by privacy and security officers because it offers details about how the actions (and failures to act) allowed an infiltration to spiral into a breach that affected 825,000 New Yorkers and 62,871 Connecticut residents, including some of XTIUM's own employees.

Yet, the actual entry point apparently remains unknown. XTIUM "did not have sufficient logging or monitoring in place to protect, detect, and defend against misuse of the remote support tool account. XTIUM's logging and monitoring of its own sign-in processes were so deficient at the time of the attack that XTIUM cannot definitively confirm how the threat actors accessed the XTIUM system," according to the settlement.

BCHP was among 18 XTIUM clients affected but the only one that suffered an actual breach.

Sometime in August 2024—the date isn't disclosed—a "threat actor" got into XTIUM's systems "through its implementation of a third party remote support tool used to service clients including BCHP. XTIUM did not implement the remote support tool utilizing all of the security measures recommended by the third party vendor," the AGs claim in the settlement.

The first BCHP learned of the infiltration from XTIUM was Sept. 6, 2024, but it may not have responded to the news until the following day when it took extremely limited action. According to the settlement, "BCHP reset all BCHP system user passwords but took no further action, such as resetting system passwords, resetting administrator passwords, or isolating the BCHP system from the internet until it could confirm no breach had occurred."

On Sept. 10, "BCHP detected unauthorized system activity and cut off internet access to the BCHP network while it investigated. BCHP was able to remediate its system and bring it back online by September 13, 2024."

The threat actors "exfiltrated an unencrypted archive of patient billing records, including patient and guarantor names, addresses, dates of birth, social security information, health insurance information, billing information, and treatment information. Employee records were also exfiltrated, containing name, address, date of birth, social security number, and driver's license number."

The settlement states that "multiple BCHP executives responsible for data security" knew the archive was unprotected for two years before the breach. Additionally, the organization failed to address "extensive findings" in a 2023 information security audit.

BCHP "failed to implement and enforce common standard security policies for its IT system, XTIUM neither requested these BCHP policies nor followed common standard practices when handling BCHP tasks for which BCHP provided no policies. As a result, XTIUM managed certain IT functions in the BCHP system using a single shared administrative account with unrestricted access and unlimited privileges," the settlement states.

As part of the infiltration, the "attacker used the shared, unrestricted XTIUM administrative account to access BCHP's system," compromising "four additional unrestricted BCHP administrative accounts. These four accounts were 'non-human service accounts' that should have been restricted in multiple ways, including barring interactive logins by humans. Because BCHP failed to adopt and enforce common standard information security policies, these accounts were used by threat actors to gain access to BCHP's entire system."

The required security enhancements in the settlement mirror those that the HHS Office for Civil Rights typically includes in corrective action plans, such as developing an information security program that includes conducting a

PATIENT PRIVACY COURT CASE (Continued)

data inventory and annual risk assessment and developing corresponding mitigation plans.

Moreover, recognizing the working relationship between BCHP and XTIUM, the settlement requires both organizations to "maintain written documentation (i) clearly identifying each entity responsible for adopting, implementing, maintaining, monitoring, and updating all elements set out in the Information Security Program, and (ii) clearly identifying the roles and responsibilities of specific individuals responsible for executing each discrete element of the Information Security Program."

Endnotes

1 Office of the New York Attorney General Letticia James, "Attorney General James and Attorney General Tong Secure $2.7 Million from Pediatric Health Network and IT Company for Failing to Protect Customer Data," news release, October 16, 2026, https://bit.ly/4e1Ylpl.

2 Letticia James, Attorney General of the State of New York, Bureau of Internet & Technology, *Assurance of Discontinuance*, Assurance No. 2026- 057, October 16, 2026, https://bit.ly/4zk3Pon.

continued from p. 2

the response, with respect to the request for a copy of Shen Smiles' internal policies and procedures evidencing compliance with 45 C.F.R. § 164.524, the response is 'None.' With respect to the request for policies and procedures evidencing compliance with 45 C.F.R. §§ 164.530(c); 164.502(a) and 164.404-408, the response is also 'None.'"

Because she did not agree to a voluntary settlement—which routinely involves a CAP—OCR moved to impose a civil money penalty (CMP). In calculating a penalty for the two violations, OCR came up with a total of $1.4 million, based on $100,000 per violation for seven years. However, it cut that down, as noted, to $140,000. This was done in consideration of "the presumed size of Shen Smiles' business, and its location in rural Pennsylvania, to avoid the alleged complete financial failure of Shen Smiles and concomitant loss of a health care provider in a rural area of Pennsylvania."

First Consideration Is 'Ability to Pay'

Iliana Peters, a shareholder in the Washington, D.C.-office of Polsinelli PC and a former OCR regulator, told *RPP* the agency's "first consideration in any settlement is the entity's ability to pay."

Adding that she could not comment on specific cases, Peters noted OCR has previously settled for "as little as $10,000, $15,000 and $30,000, in cases where I assume the entities did not have the ability to pay more. So, while the egregiousness of any potential violations [is] certainly one of the most important considerations for OCR settlements and civil money penalties, OCR does not intend to put any particular entity out of business with a settlement agreement."

RPP sent OCR a series of questions about its handling of this case, including whether the noncompliance seemed typical of small or rural providers; whether OCR had ever reduced a CMP by 90% before; whether OCR was aware of the malpractice award and whether it played into the reduction; and whether OCR reported Shen to any professional or licensing boards based on the findings in its investigation. OCR did not respond to these questions.

Court and other documents reveal more to this story than is evident from OCR's statements and some of the information directly contradicts the government.

For example, OCR repeats Shen's allegation that someone stole her records. In reality, she made that claim against Catherine Martin—Heffelfinger's sister—but she was fired by Shen before Shen claimed she took the records, Lepisto said.

During the trial, Martin denied taking the records.

Dental Assistant 'Immediately Alarmed'

Moreover, Shen changed her story numerous times about whether she had Heffelfinger's records, according to Lepisto and court documents. Shen also was accused of conditioning the records' release on Heffelfinger signing an affidavit saying she wouldn't make any claims against her, which she did not sign. Shen later said she "did not know" whether this had actually happened and said others unknown to her could have been involved, according to a deposition *RPP* viewed.

As told in the Supreme Court's dismissal of Shen's appeal, Heffelfinger had known Shen for 10 years before becoming her patient in 2013. "On May 13, 2018, Appellee went to Dr. Shen for dental care with a lesion present on the left side of her tongue. Throughout more than six visits in 2018, each initiated by Appellee, the lesion continued to grow and worsen. In each instance, Dr. Shen prescribed palliative treatment but failed to refer Appellee for specialist care, perform an oral cancer screening or biopsy for diagnosis of the lesion, nor schedule Appellee for follow-up visits. In December of 2018, Dr. Shen's then-assistant, Dora Comstock, looked for the first time at Appellee's sore, and was immediately alarmed."[3]

Comstock testified that "she raised her concern with Dr. Shen" who "responded in a hostile manner and told Comstock to stay silent. Nevertheless, Comstock instructed Appellee to immediately go to an oral surgeon. Appellee visited an oral surgeon, Niral Parikh, DDS, on December 28, 2018, who immediately recognized the lesion as possible squamous cell carcinoma, and referred Appellee for a biopsy, which

continued on p. 6

ONC 'Unleashing Prosperity' Rule Keeps Privacy, Security Certification Criteria

The HHS Office of the National Coordinator (ONC) for Health Information Technology has backed off its original proposal to "remove all the privacy and security (P&S) certification criteria in §170.315(d) and the associated Privacy and Security Certification Framework (P&S Certification Framework) under §170.550(h)," based on "the robust response from commenters and their strong views in favor of preserving" both of these, the agency said.[1]

Published Oct. 28, the Health Data, Technology, and Interoperability: ONC Deregulatory Actions To Unleash Prosperity rule finalizes a proposed regulation published Dec. 29, 2025. The final rule "includes deregulatory actions that: take into consideration suggestions and comments received" on that rule; "account for the current and future state of technology; reduce burden on health IT developers; and promote innovation for health IT developers, providers, and other interested parties."

The rule, referred to as HTI-5, goes into effect Dec. 28 for most provisions.

The proposed rule sought to "remove the P&S certification criteria and P&S Certification Framework for a multitude of reasons that led to our conclusion that the costs and burden of these certification criteria and Certification Program requirements far exceed their intended purpose and benefits," ONC explained.

The final rule reiterates five of the reasons included in the proposed rule, for example, what it called the "disconnect between health IT certified to the P&S certification criteria under the Certification Program and the implementation and compliance responsibilities of most purchasers and users of certified health IT with the requirements of the HIPAA Privacy and Security Rules."

ONC said the disconnect "led to the introduction of unnecessary regulatory burden and duplication, as well as unwarranted opportunity costs for innovation. As we noted above and in our prior rulemakings related to the P&S certification criteria, the adoption of health IT certified to the P&S certification criteria does not guarantee compliance with the requirements of the HIPAA Privacy and Security Rules."

Yet, ONC acknowledged that "the vast majority of commenters did not support" the removals.

"With limited exceptions, these commenters generally did not comment on or respond to our rationale for proposing to remove the P&S certification criteria and the P&S Certification Framework. Rather, they offered different rationales for keeping the P&S certification criteria and P&S Certification Framework. Commenters stated that certification provides a minimum baseline of P&S capabilities and a mechanism for verifying that these capabilities exist in health IT products that health care providers purchase, license, and use. Further, health care providers expressed concern that removal of the certification requirements will both shift burden to health care providers to verify the existence of the capabilities and lead to developers removing P&S capabilities due to costs and burden. These concerns were particularly acute for small and rural providers that stated they had limited resources to address these concerns and negotiate inclusion of capabilities in health IT. A few commenters asserted that privacy and security capabilities also support patient safety (*e.g.*, ensuring health information remains reliable)," the rule states.

ONC suggested removal could be revisited.

"We will continue to consider the best regulatory approach for the P&S certification of health IT under the Certification Program in anticipation of future rulemaking. This will also provide additional time to consider comments related to alignment of the P&S certification of health IT under the Certification Program with policies and requirements of the HIPAA Privacy and Security Rules," the rule states. "Future rulemaking may include proposing to remove all or some P&S certification criteria, updating certain P&S certification criteria, changing the P&S Certification Framework, or other options to address the concerns we have expressed in this rulemaking and those concerns raised by commenters."

ONC received nearly 6,500 comments on the proposed rule. Among those rejecting the P&S changes was Fairview Health System of Minnesota, which opposed what it termed the "erosion of cybersecurity standards including removal of encryption standards for authentication credentials and other standards which will put health systems at risk for cybersecurity attacks and data leakage."[2]

Overall, the HTI-5 final rule "reduces or removes certain long-standing, functionality-oriented and document-based certification criteria. These certification criteria include capabilities that are already well established in health IT products in the markets or impede innovation," ONC said in a statement on its website.[3]

Of the current "60 certification criteria within the Certification Program, the HTI-5 final rule removed 14 criteria and revised seven criteria," ONC said. The agency "retained and made no changes to 39 certification criteria, which include the new and revised criteria that were adopted in the Health Data, Technology, and Interoperability: Electronic Prior Authorization and Real-Time Prescription Benefit (HTI-4) Final Rule."

Endnotes

1 Health Data, Technology, and Interoperability: Health Data, Technology, and Interoperability: ONC Deregulatory Actions To Unleash Prosperity, 91 Fed. Reg. 67,916 (Oct. 28, 2026), https://bit.ly/3WiealY.

2 Jane Anderson, "Providers, Health Groups Urge Changes In Proposed IT Certification Program Update," *Report on Patient Privacy* 26, no. 4 (April 2026): 9.

3 Office of the National Coordinator for Health Information Technology, "Health Data, Technology, and Interoperability: ONC Deregulatory Actions to Unleash Prosperity (HTI-5) Final Rule Overview," fact sheet, October 26, 2026, https://bit.ly/4eIYHSf.

continued from p. 4

confirmed the cancer diagnosis." It was stage IV, requiring surgeries, radiation and chemotherapy and resulted in permanent speech deficits, scarring, lymphedema, fear of recurrence and other effects, according to court records.

Some Records Were Kept at Dentist's Home

The "missing" medical records were key to showing whether Shen had seen Heffelfinger or not during this period.

As the ruling states, "Dr. Shen's patient ledger did not reflect any appointments with Appellee during this timeframe, and Dr. Shen failed to maintain any medical records relative to Appellee. As a result, the trial court admitted testimony from Appellee's sister, Catherine Martin, Dr. Shen's former office manager from 2013 to 2019. Martin testified that Dr. Shen regularly took patients 'off-the-books' and received payments in unrecorded cash amounts, or in-kind services, which would therefore not have been reflected in her patient's ledger. Additionally, the trial court admitted testimony that Dr. Shen herself was responsible for the medical records relevant to the Appellee during that time frame the records went missing."

According to a news report of the jury trial, Shen denied her care was negligent and left the courtroom after her testimony and was gone for the remainder of the trial, which Lepisto said helped his case. Lepisto told a journalist he urged the jury to "render a verdict that Dr. Shen would be able to hear and feel 50 miles away in her office."[4]

Lepisto said OCR's description of Shen's practice was "accurate" and "consistent with employee testimony and former employee testimony. There was testimony from witnesses that she would bring patient records home, and oftentimes records would be strewn about her home. And there was a person who was in the home helping take care [of] her mother. She testified that there were times that she would get a call and she would need to bring records to the office from the home."

Overdue Reg May Have Provided Funds

Rather than stolen records, "there was evidence that the chart was kept in a locked area of the office that only Dr. Shen would access," Lepisto said. "There was testimony that another worker saw Mary's chart in the office after the request had been made and was scolded by Linda Shen, when she questioned her about 'wasn't this the chart that we were looking for before.'"

Yet collecting the $11.5 million the jury awarded has proved elusive. Sources of funds for Heffelfinger have been hard to come by, and, as noted, OCR hasn't helped. More than 10 years ago, Congress told OCR to implement a regulation to allow the sharing of financial penalties it collects with those affected by HIPAA violations. Because it still has not done so, the federal government would have kept all of the $140,000 Shen agreed to pay.

Beyond Heffelfinger's benefit, "a regulation that does address the victim of the potential violation, I think, would be in the public's interest, as well," Lepisto told *RPP*.

The newly Senate-passed HIPAA expansion bill championed by Sen. Bill Cassidy, R. La., contains a provision again requiring OCR to write that regulation, but the bill has to pass the House and become law before OCR would get another nudge to start this task. Cassidy himself lost his primary and will be gone by the time the new session of Congress begins in late January.

Additionally, Shen had a $1 million malpractice insurance policy, but because she did not follow notice procedures, the claim is not being paid, Lepisto said.

No Changes Mean 'Other Patients At Risk'

OCR seeking to ensure Shen stays in business with a smaller CMP cuts two ways, Lepisto said.

"Her continuing dental care puts those potential patients at harm," when OCR instead could have been monitoring her practice and requiring changes, he said.

"Shen just did not follow the standard of care of doing any sort of cancer oral examination to rule out any concerning lesions or cancer," Lepisto said. "And I do think that part of the problem was, again, the record keeping. She didn't have a standard office visit note. The testimony was that she would just write things down on pieces of paper and then maybe put it into the chart or maybe fill something out later."

Heffelfinger, "theoretically, benefits from Dr. Shen continuing to practice because she should be earning money, which should go to Mary Heffelfinger. However, she's a little conflicted because she knows that Dr. Shen continuing to practice, again, puts other patients at risk," he added. ✧

Endnotes

1 U.S. Department of Health and Human Services, "HHS' Office for Civil Rights Settles HIPAA Privacy Rule Investigation With Dr. Linda L. Shen/D/B/A Shen Smiles, P.C." news release, October 8, 2026, https://bit.ly/4efhIM2.

2 U.S. Department of Health and Human Services, "Notice of Proposed Determination - Dr. Linda L. Shen D/B/A Shen Smiles, P.C.," July 31, 2024, content last reviewed October 8, 2026, https://bit.ly/4zliQGa.

3 Heffelfinger v. Shen, No. 681 MDA 2024 (Pa. Super. Ct. July 21, 2025), https://bit.ly/4A6FmTs.

4 "Jury Hits Pa. Dentist With $11M Verdict for Delayed Cancer Diagnosis, Alleged Cover-Up," *The Legal Intelligencer,* February 23, 2024, https://bit.ly/47OsFAy.

OCR's Noonan Shares SUD Complaint, Breach Data, No Guesses on Privacy Reg

The wait continues for the final revised Privacy Rule, but it should be released "in the near future" and will embrace "some" of the provisions in the now five-year-old proposed regulation. Meanwhile, the estimate for the final Security

Rule remains next July and the timing for the results of the HHS Office for Civil Rights' (OCR) second round of audits (remember those?) is perhaps two years away.

These are among the updates Timothy Noonan, OCR deputy director for health information privacy, data and cybersecurity, shared at the recent Health Care Enforcement Compliance Conference on Oct. 28. He also disclosed that the agency has received more than 800 complaints of HIPAA-like violations of substance use disorder (SUD) records under regulations known as Part 2.

During his hour-long talk, Noonan addressed a range of other issues, including OCR's ongoing investigations into healthcare systems' possible violations of access requirements, related particularly to parental rights.[1]

Of note: in reviewing OCR's breach data, Noonan said that last year, OCR received 804 reports of "large" breaches, those affecting 500 or more individuals, and said that breaches of all sizes affected 140,575,464 people.

This is nearly 100 million more than OCR Director Paula Stannard reported during the agency's joint National Institute of Standards and Technology conference. Stannard's data showed 650 large reports and an overall total for 2025 of 45,675,743 people affected.[2]

OCR's explanation is that totals change when covered entities (CEs) or business associates amend breach reports.

Back to regulatory updates, Noonan noted that the revised Privacy Rule is still under review by the Office of Information and Regulatory Affairs (OIRA), part of the Office of Management and Budget, as it has been since April 2. OIRA's website also contains the government's plan for upcoming regulations, typically updated twice yearly. Noonan referred to the most recent version as the "spring" agenda, but that is not how it is titled. Posted July 3, the agenda refers simply to 2026. It lists August for publication of a final Privacy Rule, which obviously did not happen.

Privacy Reg Content, Release Date Unknown

Complicating the rulemaking is that OCR apparently intends to revise the time frame for CEs to respond to a patient's request for records more significantly than would be allowed under regulations. It proposed shortening the 30-day requirement to 15, but the regulatory update showed a new proposed rule centered solely on access. This has led to speculation that OCR will reserve or omit those provisions so they can be revisited in a new rule that presumably will shorten the 15 days.[3]

Noonan noted that the proposed rule "sought to improve health information sharing for more effective healthcare, empower individuals with their own health information and lift unnecessary burdens on covered healthcare providers and health plans."

The proposed rule also would "strengthen the individual's rights to access their own health information, including electronic information; improve information sharing for care coordination and case management for individuals; facilitate greater family and caregiver involvement in the care of individuals experiencing emergencies or health crises; and reduce administrative burdens on HIPAA covered providers and health plans while continuing to protect individuals' health information, privacy interests," he said.

"We do anticipate publishing a final rule in the near future, finalizing some of the proposals that we had proposed back in 2021," Noonan said, without hinting at what's in the proposed rule that might not make it into the final one.

Noonan also reviewed some provisions in the proposed revised Security Rule and noted that a final rule has been moved to long-term actions in the regulatory update, with an expected publication date of July 2027.

OCR Reviewing SUD Records Complaints

With regard to SUD records enforcement, the final rule that harmonized HIPAA with regulations at 42 CFR Part 2 was published on Feb. 16, 2024, with a two-year compliance period. OCR began exercising its authority on Feb. 16, which was also the same day the agency started accepting complaints of possible violations of applicable privacy, security and breach notification requirements.

OCR has not issued any settlements or other enforcement actions regarding SUD records, but it has received "somewhere between about 850, 900" complaints, according to Noonan.

"We're reviewing them and we'll be initiating investigations and such, just as we do [with] HIPAA enforcement," said Noonan. He pointed out that in September, OCR published guidance for Medicaid agencies related to records access for the purposes of verifying work requirements and said the audience should "stay tuned for future announcements on what we're doing with Part 2."

Source of Breaches Changed Little

Turning to reports of breaches affecting 500 or more individuals, "there was a 12% increase from 2021 to 2025, going from 715 to 804," he said, with "about an 8.5% increase from [20]24 to [20]25. Also noteworthy for 2025, there was a drop in the number of individuals affected by large breaches, although, I have to say that wasn't much of a surprise given that 2024 was, is a record with 290 million individuals affected by large HIPAA breaches."

Reviewing data so far this year, as of the end of September, OCR had received 558 large breach reports affecting "nearly" 77 million people, Noonan said. "I should point out, though, the data does continue to change, particularly for 2025."

Annual data is "continuously updated as breaches are reported, verified, and then it is often the case, during the

course of the investigation, the covered entity may file an addendum updating OCR on the number of individuals affected," he added.

Looking at the location of breaches, "the key takeaway here is network servers and email account[s] for 88% of the large breaches reported to OCR," Noonan said. "This has been consistent over the last several years."

Reviews Continuing of Thwarted Parental Access

Moving on to records access, Noonan recalled that OCR initiated this enforcement program in 2019 and continues to take action, most recently settling noncompliance allegations with a dentist in Pennsylvania.

RPP is exclusively reporting that the complaint leading to this $140,000 settlement came from a malpractice attorney who was shocked to hear of the settlement. He told *RPP* his client has been unable to collect on an $11.5 million negligence award the dentist was ordered to pay following a jury trial and subsequent unsuccessful appeals related to cancer the dentist failed to acknowledge. The attorney said he wishes OCR had required corrective actions, which could have freed the $140,000 to be paid to his client (see story, p. 1).[4]

OCR also previously announced, via a December "Dear Colleague Letter," that it was conducting compliance reviews into health systems related to parents' right to access their minor children's medical records, Noonan said. He did not share the status of these reviews, when findings might be released or in what form.

Audits to Conclude With 'Industry Report'

As previously mentioned, Noonan touched on OCR's audit program, which he acknowledged typically generates "a lot of questions," but he shared few specifics.

OCR's first round of audits took place 10 years ago, the results of which were released in 2020. OCR began a second round in December 2024, looking at "selected auditees' compliance with the key provisions in the Security Rule best situated to defend against" hacking and ransomware, he said.

"As with the audits that we did back in 2016, when these audits are done, we anticipate publishing an industry report, which will provide some general information to the public on our findings with respect to the audited entities," Noonan said. OCR officials "would anticipate publishing [the industry report], I don't know if it'll be next year, but certainly within the next two years." ✧

Endnotes

1 Timothy Noonan, "Update from the HHS Office for Civil Rights," HCCA Healthcare Enforcement Compliance Conference, October 28, 2026.

2 "Office for Civil Rights (OCR) Breach Data," *Report on Patient Privacy* 26, no. 10 (September 2026): 4.

3 Theresa Defino, "OCR Director Says Carry On: Usually Sleepy July Sees News of Security Delay, Surprise Access Reg," *Report on Patient Privacy* 26, no. 8 (August 2026): 1, https://bit.ly/4eD5f4O.

4 Theresa Defino, "Access Complaint By Lawyer Triggered $140K OCR Deal With Dentist; $11M Award's Unpaid," *Report on Patient Privacy* 26, no. 11 (November 2026): 1.

Multistate Labcorp Settlement Called 'Roadmap' for CEs to Manage Vendors

Covered entities (CEs) can't outsource their responsibility for guarding protected health information (PHI), even when that PHI is being handled by a vendor. That's the message at the heart of a $2.3 million settlement between the Laboratory Corporation of America (Labcorp) and state attorneys general (AGs) that resolves a 2019 data breach at Labcorp's debt collector.

At the same time, Labcorp's recent settlement provides the industry with "a detailed, practical roadmap for vendor oversight" to help meet that responsibility, Shalyn Watkins, senior counsel at Holland & Knight LLP, also explained.

"Overall, the settlement gives organizations a constructive framework for continuing to improve their vendor oversight programs," Watkins told *RPP*. "Companies that take these steps now will be well positioned to protect patient data and to show regulators that their programs are thoughtful."

Breach Impacted 27.5M

The settlement resolves a breach at Retrieval-Masters Creditors Bureau, doing business as American Medical Collection Agency (AMCA), that potentially exposed the personal information of more than 27.5 million individuals throughout the United States, including 10.2 million Labcorp patients, according to Connecticut AG William Tong, who led the multistate coalition.[1]

A multistate coalition of AGs settled with AMCA in 2021 after the company's bankruptcy petition was dismissed. The coalition in the September Labcorp settlement includes 43 states and the District of Columbia; California, Louisiana, Mississippi, Montana, North Dakota, South Dakota and Wyoming did not participate in the September agreement.

Tong pointed out that the data breach occurred at AMCA; however, the data involved was the sensitive data of Labcorp patients, adding, "while companies can contract with vendors freely and delegate authority, data security is a non-delegable duty. Vendor management remains one of the most challenging areas in cybersecurity, but it is critical that businesses properly vet their vendors and ensure that information shared with those vendors will be kept secure."

The multistate settlement provides what Tong described as "strong requirements around vendor management, especially medical debt collection." These include:

- Strengthening the company's information security program, including "an incident response plan that includes internal reporting of vendor security events;
- "Minimizing the sharing of data with vendors while balancing certain needs of debt collectors to meet their legal obligations;
- "Expanding the vendor risk management program to include requiring a dedicated team, employing tools to evaluate vendors, and verifying vendor compliance;
- "Adding specific requirements for debt collectors as a specialized subset of vendors, including maintaining contract inventories, enforcing cybersecurity standards through contract, segmenting data which is often aggregated by debt collectors for multiple clients, and requiring debt collectors to perform assessments and audits, and including the right of termination for noncompliance; and
- "Hiring a Third-Party Assessor to perform an information security assessment with a focus on vendor risk management."

As part of the settlement, Labcorp will make a $2.287 million payment to the 44 jurisdictions in the coalition, Tong said, adding that the payment will supplement a multistate settlement with AMCA, which included a $21 million suspended payment due to the company's bankruptcy.

Labcorp also has agreed to pay $35 million to settle class action litigation arising from the AMCA breach. A federal court approved that settlement in August. The broader litigation, which also involves other healthcare organizations that used AMCA, remains ongoing.[2]

Settlement 'Reinforces Obligations'

Watkins noted that the settlement agreement "is not a finding of fault" and that Labcorp entered into the settlement agreement "without any admission of liability or wrongdoing and without any adjudication of fact or law." She added that "the 2019 incident happened at a debt collection vendor, not within Labcorp's own systems."

In addition, Watkins said that the settlement largely reinforces existing obligations rather than creating new ones. For example, she said that business associates handling electronic PHI (ePHI) for CEs already have to secure that ePHI under the HITECH Act, and that many of the terms contained in the settlement "come straight from existing HIPAA concepts," including BA agreements and the minimum necessary standard.

"What stands out is how specific it is," she said. "The [Assurance of Voluntary Compliance] lists concrete safeguards, such as an incident response plan that covers vendor security events, a dedicated vendor risk management team, risk-based vendor monitoring and debt-collector-specific contract terms. That gives organizations a useful benchmark for evaluating and improving their own programs."

The AGs said that while companies can contract with vendors and delegate authority, data security is a non-delegable duty, Watkins said. At the same time, "they also acknowledged that vendor management remains one of the most challenging areas in cybersecurity. That acknowledgment matters, because even organizations with well-run programs cannot control every risk inside a vendor's environment."

Ongoing Oversight Expected

In practice, Watkins said she reads the "non-delegable" message "as a call for ongoing oversight, not a guarantee of perfect outcomes. A strong contract is the starting point. Regulators also want to see that the organization verifies what vendors tell it, follows up on findings and has a plan for when something goes wrong. The Assurance reflects this."

She explained that the document calls for corroborating vendor questionnaire responses where appropriate, requiring annual attestations that critical or high-risk deficiencies have been or will be addressed and defining in advance the roles of the company and the vendor in a security event, including who sends consumer notices.

"Organizations that document these steps will be in a much stronger position if a vendor has an incident despite everyone's best efforts," Watkins said.

Watkins identified two aspects of the agreement that she said she found particularly noteworthy.

"First, the assurance takes a risk-based approach," she said. "The frequency, type and depth of vendor monitoring depend primarily on each vendor's risk rating. That is a practical model because it lets organizations focus resources where the risk is highest instead of treating every vendor the same way." The definition of "vendor" also excludes third parties that handle only de minimis amounts of consumer data, she said.

Second, Watkins explained, "the debt collector provisions are notably detailed. They require a contract inventory with risk ratings, contractual adoption of industry-recognized frameworks such as the NIST [National Institute of Standards and Technology] Cybersecurity Framework, data segmentation in multi-tenant environments where feasible, key management and NIST-aligned data disposal requirements, annual risk assessments and penetration tests" and other audits and assessments, including by HITRUST.

At the same time, the terms build in flexibility, Watkins said. For example, in situations where segmentation isn't feasible, alternative reasonable measures may be used, she said.

Watkins expects regulators to look at these provisions "as a reference point" for evaluating vendor oversight in the future. "Organizations can also use them now as a constructive benchmark," she said, noting that "many of the obligations

expire five years after the October 1, 2026, effective date, which signals a focus on building lasting program improvements rather than imposing permanent obligations."

Lasting Improvements Targeted

The settlement shows that state AGs continue to play an active role in healthcare privacy and security, Watkins said. "For healthcare organizations, the practical point is that HIPAA compliance should be viewed together with state law obligations. A coordinated, cooperative approach with regulators is also valuable."

For example, the settlement includes a meet-and-confer process that gives Labcorp 30 days to respond in good faith to any compliance concern before enforcement, Watkins said. It also provides for the third-party assessor's report to be treated as exempt from public disclosure to the extent state law permits. "Features like these show how multistate resolutions can be built to support continued compliance and constructive dialogue."

However, Watkins said it's not clear whether state AGs will join in this type of settlement on a regular basis. "Labcorp is uniquely situated throughout the United States in ways that many companies are not," she said. "What I believe we are learning here is that when you have a national platform, multistate enforcement is not off the table. States can coordinate efforts with the federal government when they see fit." ✧

Endnotes

1 Connecticut Office of the Attorney General, "Attorney General Tong Leads $2.3 Million Multistate Settlement with Labcorp Over the American Medical Collection Agency Data Breach," news release, September 24, 2026, https://bit.ly/4zI7ZGg.

2 In re: American Medical Collection Agency, Inc. Customer Data Security Breach Litigation, No. 19-md-2904 (D.N.J.), Labcorp settlement documents, Kroll, https://bit.ly/4z2bvvc.

TEFCA Disruption After Update Prompts Broad Complaint from Consumer Group

A change to requirements for exchanging health information under the Trusted Exchange Framework and Common Agreement (TEFCA) disrupted patients' ability to access their records through third-party applications, prompting criticism of the rollout and calls for improved coordination, testing and oversight.

The Sequoia Project, the recognized coordinating entity (RCE) responsible for administering TEFCA, acknowledged that implementation problems stemming from the Oct. 1 rollout interrupted access but maintained that nearly all impacted exchange volume has been restored.

The disruption followed implementation of specific technical requirements contained in version 3.0 of TEFCA's individual access services (IAS) standard operating procedure, which the Sequoia Project said was intended to make patient identification more reliable and improve responsiveness to requests for health information.

The changes affect how qualified health information networks (QHINs), which connect participating organizations under TEFCA, process requests from applications that patients authorize to retrieve their health information.

As *RPP* previously reported, in June HHS announced that the Office of the National Coordinator (ONC) for Health Information Technology awarded a new contract to strengthen oversight of the network and verify that organizations participating in TEFCA comply with required policies and procedures. ONC is also conducting additional reviews of qualified QHINs and their participants to assess compliance with TEFCA rules and operating requirements.[1]

A new version of the IAS was the subject of complaints by the American Hospital Association (AHA), which urged the Sequoia Project to delay implementation of new patient-matching methodologies that bypass or limit provider verification. Prior to implementation, AHA argued that it could "expose hospitals to unauthorized disclosures, data breaches and misidentification errors."

However, the change went ahead and compliance was required by Oct. 1—after which problems began immediately.

CARIN: Is a New RCE 'Needed?'

On Oct. 12, the Creating Access to Real-time Information Now through Consumer-Directed Exchange (CARIN) Alliance, a coalition advocating for consumer-directed access to health information, sent a letter to ONC and the RCE that it shared on LinkedIn. "Due to the heroic efforts of a handful of QHINs and [Connected Service Providers] who self-organized, much of that access has been restored, but 12 days later, there are still QHINs who are not compliant with the changes that were required to be implemented by 10/1. This means millions of patients still do not have access to their own health information on TEFCA," it said in the post.[2]

The letter asked both the RCE and ONC to "make immediate changes to how TEFCA is organized, staffed, and managed to ensure this does not happen again. We also recognize production issues may occur, but the RCE's lack of prioritization related to this issue over the last 12 days when millions of patients are waiting to access their own health information is inexcusable."

CARIN said the problems were predicated and that several QHINs were unprepared for the changes. "We ask the RCE and ONC to treat this outage as an ongoing critical incident and to take immediate action to restore reliable IAS exchange."

The organization listed 10 "immediate suggested actions," including "creat[ing] a temporary, clearly bounded warning period—for example, 30 days—during which signature checks remain in force while specified token-format errors are logged and flagged rather than rejected." It also suggested "defin[ing] which errors qualify for warning treatment, which errors continue to require rejection, who may authorize the temporary policy, and the conditions for ending it" and "strength[ing] technical architecture and testing leadership."

"If the RCE cannot establish these capabilities promptly, ONC should evaluate whether changes to the RCE's responsibilities, staffing, or designation are necessary including whether a new RCE is needed," the alliance said.

CARIN spokesperson Ryan Howells told *RPP* that applications involved in the alliance, such as those listed on MyHealthApplication.com, which is run by CARIN, and the Medicare App Library, collectively support access for millions of patients.

It is not known whether ONC responded to CARIN's letter.

RCE 'Working Diligently to Restore Access'

However, a week later, the RCE acknowledged that inconsistent technical implementations among QHINs had caused connectivity problems, including differences in how networks verified IAS claims tokens used in identity verification.

"There were incompatibilities and different levels of readiness across the QHINs for the Oct. 1 change that led to some lost connectivity," the RCE said in an Oct. 27 update. "While the QHINs had engaged in partner testing ahead of Oct. 1, [that testing] did not uncover differences such as varying levels of rigor in applying technical constraints. The RCE will leverage lessons learned to prevent any future disruptions to the network."[3]

In a statement provided to *RPP*, the RCE said it and ONC "are committed to the success of TEFCA, including enabling consumer-directed access" via IAS. "We recognize any outage is a disruption to the patients and providers…and have been working diligently to restore IAS services."

The RCE said that all QHINs were supporting the latest IAS requirements and that full IAS activity had been restored as of Oct. 26.

The RCE also issued a compliance bulletin clarifying requirements and addressing questions raised during implementation. It did not answer specific questions about how many QHINs or IAS providers were impacted or whether any individual access problems remained unresolved.

CARIN Criticizes NDAs

CARIN maintained that the disruption exposed broader problems with TEFCA governance: Howells specifically cited coordination, advance testing and more effective oversight of changes affecting all QHINs as continuing challenges.

The organization also criticized nondisclosure agreements (NDAs) involving TEFCA participants.

"TEFCA is the way all networks…will ultimately exchange health data," Howells said. "We believe if that is the goal, it requires a level of coordination and transparency (both when things go well and when things don't go well) that is woefully lacking today. We believe one of the causes for that lack of transparency is the NDAs that have been signed by those participating in TEFCA."

Asked about CARIN's criticisms, the RCE said it remains committed to collaboration and transparency, including seeking industry and public feedback during TEFCA's change management process.

"The recommendations of the CARIN Alliance and all of the feedback from the TEFCA community will be taken under review and consideration on how to further enhance our framework for the patient good," RCE spokesperson Dawn Van Dyke told *RPP*.

She did not directly address questions about CARIN's concerns regarding the NDAs and how those might have impacted participants' ability to discuss the disruption publicly. ✧

Endnotes

1 Jane Anderson, "Amid Growth, Sequoia Shifts TEFCA Focus to Operations, Compliance Checks," *Report on Patient Privacy* 26, no. 10 (October 2026): 8.

2 CARIN Alliance, LinkedIn post, October 13, 2026, https://bit.ly/3Uvo6bh.

3 The Sequoia Project, "Current Status of Efforts to Fully Implement Individual Access Services SOP version 3.0," announcement, updated October 27, 2026, https://bit.ly/4eB1c98

PRIVACY BRIEFS

◆ **Federal and South Carolina officials have launched a six-month pilot program designed to strengthen cybersecurity at rural hospitals, providing participating facilities with technology and technical assistance at no cost**. Project Lifeline 250, announced Oct. 26 by South Carolina Republican Gov. Henry McMaster and White House National Cyber Director Sean Cairncross, will bring together federal and state agencies and private technology companies to help hospitals identify vulnerabilities, strengthen network defenses and maintain patient care during cyberattacks. The initiative will focus on identifying and replacing high-risk or outdated medical devices and other technology. It will

Contact Paule Hocker at paule.hocker@corporatecompliance.org or 888.580.8373 to find out about our reasonable rates for individual and bulk subscriptions.

PRIVACY BRIEFS

also help rural hospitals deploy backup systems that can support critical hospital operations following a cyber incident, enabling hospitals to continue providing care despite any disruption. South Carolina law enforcement and private-sector partners, including Microsoft, Cisco, Trellix and Zscaler, are also involved in the pilot project. Officials plan to evaluate whether the cybersecurity technologies and approaches tested via the pilot can be expanded to hospitals and other critical infrastructure nationwide. The initiative builds on Project Watershed 250, a similar cybersecurity pilot involving water and wastewater systems in Texas.[1]

◆ **More than one-quarter of healthcare websites failed basic privacy tests, with many continuing to transmit information to advertising and social media companies despite visitors' privacy preferences, according to a study released Oct. 28 by website privacy testing company DataTrue**. Although these tests are particularly relevant to compliance with California privacy law, they also have nationwide implications as other states adopt similar requirements and healthcare organizations face continued scrutiny over their use of website tracking technologies. The company examined 242 heavily visited U.S. websites, including 50 healthcare websites, in mid-October. Researchers tested whether the sites contacted advertising companies before site visitors made privacy choices, whether they provided clear options to reject tracking, and whether they honored Global Privacy Control (GPC) signals, which communicate users' preferences against the sale or sharing of their information. Of the 50 healthcare websites, 18 contacted advertising or social media companies before visitors made a privacy choice. Fourteen of those sites did not change their tracking behavior when GPC was enabled, while two reduced tracking and two stopped it entirely. The study also found that 32 healthcare websites offered no apparent option to reject tracking, while nine initiated session-replay technology before visitors made a choice. Session-replay tools can record website visitors' clicks, scrolling and other interactions. Healthcare websites had the lowest overall failure rate among the five industries studied, at 28%, but performed worst at responding to GPC signals among sites that used advertising technologies. DataTrue recommended that organizations provide clear privacy choices, ensure tracking technologies honor those choices and regularly test whether information continues to be transmitted after visitors reject tracking.[2]

◆ **Four vulnerabilities found in HAPI FHIR, an open-source software framework used to exchange healthcare information, could expose patient records or disrupt services, according to an Oct. 22 advisory from the National Institute of Standards and Technology, using information provided via the Cybersecurity and Infrastructure Security Agency**. The vulnerabilities could allow an authorized user to access or modify records belonging to another organization, disclose patient information outside a user's permitted access, or cause a denial-of-service attack without authentication, researchers warned. Two of the vulnerabilities are rated high severity, with scores of 8.1 and 7.5 on the Common Vulnerability Scoring System. Independent security researcher Abhinav Agarwal demonstrated the flaws in HAPI FHIR version 8.10.0. The software is used in multiple healthcare applications, and at the time of the disclosure, three of the four vulnerabilities had no available fixes, although some risks could be mitigated through access controls and restrictions on compressed requests. Organizations using HAPI FHIR were urged to review their configurations and monitor vendor guidance for patches.[3],[4]

◆ **An Oct. 26 cyberattack at the University of New Mexico Health Sciences Center forced the health system to divert ambulances for two hours and suspend outpatient surgeries and appointments**. University officials said information technology teams began containing the incident after detecting a threat around 11 a.m. The attack affected some employee devices but did not penetrate core networks or servers, according to the university. Hospital officials activated an emergency operations center and diverted ambulances to other hospitals from 12:30 p.m. to 2:30 p.m. Systems were restored in phases, and normal clinical operations resumed Oct. 27, according to the facility. In an Oct. 28 update, the university said it had made no concessions to those responsible for the attack, and warned patients, employees and students against responding to anyone claiming responsibility. State and federal law enforcement agencies are investigating the incident, the university said.[5]

Endnotes

1 South Carolina Office of the Governor Henry Dargan McMaster, "Gov. McMaster, White House National Cyber Director Cairncross Launch Project Lifeline 250 to Strengthen Cybersecurity at South Carolina Rural Hospitals," news release, October 26, 2026, https://bit.ly/4iMiG4P.

2 DataTrue, "The Consent Gap," October 2026, https://bit.ly/4ByEjNq.

3 National Institute of Standards and Technology National Vulnerability Database, "CVE-2026-113875 Detail," last modified October 23, 2026, https://bit.ly/4yOlao2.

4 Abhinav Agarwal, "HAPI FHIR Authorization Findings in HAPI FHIR," technical disclosure, updated October 22, 2026, https://bit.ly/4i8JhZK.

5 University of New Mexico, Health Sciences News, "UNM Warns Public Not to Engage with Any Groups Claiming Responsibility for Cybersecurity Threat," news release, October 28, 2026, https://bit.ly/4iboLYt.