American Association of Healthcare Administrative Management

Empowering the future of healthcare revenue cycle excellence.

Volume 25, Issue 10 **June 14, 2024**

Currents: AAHAM government affairs e-mail newsletter

In The News

- London Hospitals Knew of Cyber Vulnerabilities Years Before Hack
- US Health Spending Grew 7.5% to Nearly $4.8 Trillion in 2023

Legislative/Regulatory

- Insurers Still Losing in Surprise Billing Arbitration, Data Show
- IRS Plans More Nonprofit Hospital Audits as Scrutiny Heats Up
- Medicare Updates Star Ratings That Inform Insurers' Payments
- Lawmakers Take Aim at PE Health-Care Binge
- Medicare Report to Congress Highlights Program Challenges, Goals
- UnitedHealth Hack Fuels Bids to Shield Americans' Medical Data
- Medicaid Fraud Singled Out as Program Costs Approach $1 Trillion
- Biden Moves to Bar Medical Debt From Consumer Credit Reports
- Medicaid Advisers Urge Enhanced Transparency, Care Coordination

Legal

- HHS Asks Court to Deny Florida Bid to Block Transgender Care
- Tempus AI Copied Guardant Patents to Create Tests, Lawsuit Says
- Court Split Spells Trouble on Surprise Billing Award Enforcement
- High Court Agrees to Revisit 2022 Medicare Payment Ruling

Around the States

- New York: Former Opioid User Revives Disability Bias Suit Against Hospital
- North Carolina: FTC Loses Bid to Block Novant Health $320 Million Hospital Deal

IN THE NEWS

London Hospitals Knew of Cyber Vulnerabilities Years Before Hack

A group of London hospitals struggling to contain the fallout from a cyberattack against a critical supplier had known for years about weaknesses that left them vulnerable to hacks, according to documents reviewed by Bloomberg News.

The Guy's and St Thomas' NHS Foundation Trust, which runs five major hospitals in the London area, has failed to meet the UK health service's data security standards in recent years and acknowledged as recently as April that "cybersecurity remained a high risk" to its operations, according to publicly available documents that outline board of directors' meetings.

In January, the board of directors raised questions about the security of digital links between hospital computer systems and those of third-party companies.

Hackers last week brought down the trust's pathology services provider, Synnovis, with severe knock-on effects at hospitals. Doctors have, among other things, been forced to delay medical operations, postpone blood tests and resort to handwritten records. The attack has disrupted blood services so drastically that medical facilities are asking the public for donations, and one hospital is calling on its own staff to contribute.

The April report proposed an audit to identify where improvements could be made. It's not clear if improvements took place before the hack on June 3, or whether the vulnerabilities identified in the board of directors' reports — which include dated IT systems and hardware devices — had any bearing on the ransomware infection at Synnovis.

"The trust takes cybersecurity very seriously and this includes arrangements with third parties," Guy's and St Thomas' NHS Foundation Trust said in a statement. "We are working closely with partners to fully understand how this hack happened." The trust declined to comment on the cybersecurity warnings raised prior to the attack.

UK-based Synnovis is jointly owned by Synlab UK & Ireland and two publicly funded NHS trusts – Guy's and St Thomas' NHS Foundation Trust and the King's College Hospital NHS Foundation Trust – that run several hospitals in London and Kent.

The hack on Synnovis has primarily affected patients of Guy's Hospital, St Thomas' Hospital, King's College Hospital and primary care in southeast London, Bloomberg News has reported.

The impact of the breach is ongoing.

Electronic patient records are still accessible to doctors, according to a blood transfusion specialist who works with multiple hospitals in London, who spoke on condition of anonymity as they weren't authorized to share information with the media.

But a software tool that Synnovis uses to transfer blood test results into patient records is no longer functioning because of the attack, leaving an information blind spot that has caused major disruption across the affected hospitals and forced them to run at about 10% to 15% of normal capacity, the person said.

Years of cybersecurity concerns

Since at least mid-2021, concerns have been aired about cybersecurity vulnerabilities affecting hospitals operated by the Guy's and St Thomas' NHS Foundation Trust, according to the board meeting documents.

For instance, minutes from a meeting in May 2021 warned that a "significant number" of the trust's IT systems and hardware devices were "out of support or at the end of life, and which can increase the risk of cyberattack." A report in April 2022 said work had been undertaken to "partially mitigate" security risks, such as outdated Windows software, through "tactical fixes." But the report added that "some areas of the trust remained vulnerable to a cyberattack."

The trust later embarked on a program of modernizing its IT infrastructure, updating computers and carrying out simulated hacks to test for vulnerabilities. In October 2023, the trust rolled out a new electronic patient record system and began implementing a new computerized system called Blood Track to manage blood transfusions, according to the documents.

Even so, the trust's board of directors continued to raise concerns. In January 2024, the trust's IT infrastructure was said to be "configured to a good standard," but directors questioned whether sufficient security procedures were in place to monitor interfaces with third parties - such as the pathology business unit operated in collaboration with Synnovis.

Little information about the King's College Hospital NHS Foundation Trust's cybersecurity practices is publicly available. Last year, the UK's information watchdog, the Information Commissioner's Office, audited the trust and flagged that it had issues with data protection compliance. The trust had "considerable scope for improvement" to ensure it was protecting personal data, the commissioner's office found. A September 2023 board of directors' report from the King's College Trust said it had recorded "an increase in data breaches," though it's unclear whether these were related to cybersecurity incidents.

A spokesman for King's said that the ransomware attack had affected Synnovis and that there was no evidence that it had infiltrated King's systems. The prior data breaches highlighted in its board of directors' report were unrelated to the latest incident, the spokesman added.

"Data security is a priority for the trust, and something we take very seriously," the spokesman said. "Data breaches are rare, but when they do occur, we ensure they are fully investigated, and action taken to strengthen the processes we have in place."

Russian group suspected of attack

The cyberattack on Synnovis is suspected to have been carried out by a Russian-speaking ransomware gang known as Qilin, which has claimed more than 100 attacks on companies and organizations across a range of sectors since late 2022, according to the cybersecurity firm Secureworks. A representative of the Qilin gang didn't respond to requests for comment.

Ransomware gangs typically gain access to victim computers by exploiting a software vulnerability, luring a victim into clicking a malicious link in an email or using stolen credentials to log in. They then gain access to internal networks and use malicious software to encrypt files on computers, rendering them inoperable. The gang demands payment to unlock the computers and may also threaten to publish stolen data online.

"Ransomware groups that are willing to target the health-care sector understand the value of the data and also the importance of access to that data," said Cian Heasley, threat lead at Adarma Security. "As we can see from the situation affecting London hospitals, the potential leaking of stolen data is only part of the problem; the data itself is vital to patient treatment."

The breach is the third known ransomware case in the last year to have affected a branch of Synlab AG. In June 2023, the hacking gang Cl0p targeted the company's French subsidiary. In April 2024, the operations of Synlab's branch in Italy were disrupted by another ransomware gang, known as Black Basta.

In a statement last week, Synnovis said all its IT systems had been affected by the hack and that it was working with experts to resolve the issue.

"We take cybersecurity very seriously at Synnovis and have invested heavily in ensuring our IT arrangements are as safe as they possibly can be," said Mark Dollar, chief executive officer of Synnovis. "This is a harsh reminder that this sort of attack can happen to anyone at any time and that, dispiritingly, the individuals behind it have no scruples about who their actions might affect."

US Health Spending Grew 7.5% to Nearly $4.8 Trillion in 2023

National health-care spending grew an estimated 7.5% to nearly $4.8 trillion in 2023 and is projected to outpace growth in the gross domestic product over the next decade, according to national projections released Wednesday.

Increased use of health services, fueled by a record-high 93% of Americans with health coverage, drove last year's rise in spending, according to the annual report on long-term health-care costs and coverage from the Centers for Medicare & Medicaid Services' Office of the Actuary.

But from 2027 to 2032, health-care inflation, and increased use of services, are expected to push total health-care spending to nearly $7.7 trillion in 2032. That would drive the share of GDP devoted to health-care spending to 19.7% by 2032, up from 17.3% in 2022.

Total health-care spending growth is projected to average 5.6% a year from 2023 to 2032 compared to a nominal GDP growth rate of 4.3% over that period.

Legislation enacted after the Covid-19 public health emergency will influence health-care spending and insurance enrollment throughout the 10-year projection period. For example, Medicaid enrollment is expected to decline from a record 91.2 million in 2023 to 79.4 million in 2025, due to expiration of continuous enrollment provisions of the Families First Coronavirus Response Act of 2020.

And in 2026, an estimated 7.3 million people—19.2%—are expected to lose their individual marketplace coverage, or "direct-purchase insurance," due to the projected expiration of marketplace subsidies offered through the Inflation Reduction Act.

Other provisions of the IRA are expected to lower the growth rate for Medicare prescription drug spending by nearly 11 percentage points to 2.6% in 2025, said Jacqueline Fiore, a CMS economist, during an afternoon web press briefing. That's when a new manufacturer discount for low-income beneficiaries takes effect and increases the share of costs paid by drug manufacturers. Those savings, however, would be partially offset by the IRA's $2,000 cap on Part D out-of-pocket drug spending, which also takes effect in 2025 and shifts costs from beneficiaries to Medicare, the report said.

In 2026, the IRA's Medicare drug price negotiations are slated to take effect. During the initial years of negotiation, affected drugs are expected to have higher rebates that are shifted to the point of sale, the report said. "A key effect of this outcome is reduced Medicare beneficiary out-of-pocket spending, along with

increased federal spending on prescription drugs. Correspondingly, the growth rate for Medicare prescription drug spending is projected to rise sharply to 12% in 2026," the report said.

Other key findings:

- Medicare's projected 10-year average spending growth rate of 7.4% from 2023 to 2032 is the highest among major payers, including private health insurance, at 5.6%, and Medicaid, at 5.2%. The numbers reflect Medicare's projected 2% annual enrollment growth through 2029 as more aging baby boomers join the program.
- Medicaid spending, projected to fall this year because of major enrollment losses, is expected to rebound through 2025–26 as enrollment growth rates stabilize.
- Private health insurance spending growth should fall from 8.1% in 2024 to 5.3% in 2025, and then to 2.4% in 2026. That's due mainly to falling marketplace plan enrollment premium tax credits provided under the IRA expiring.

LEGISLATIVE/REGULATORY

Insurers Still Losing in Surprise Billing Arbitration, Data Show

Medical providers continue to beat out insurers in most surprise billing arbitration disputes, often pocketing awards of at least double the in-network rate for a given service, according to new federal agency data.

Providers were the prevailing party in about 82% of payment determinations made in No Surprises Act arbitration in the second half of 2023, according to a data report released Thursday by the Centers for Medicare and Medicaid Services. A total of 125,478 disputes resulted in award decisions in that period, the report showed, a 50% increase from the first half of 2023.

The 2021 surprise billing law established an arbitration process for resolving payment disputes between providers and health plans, preventing them from billing patients for emergency out-of-network care or certain out-of-network providers at in-network facilities. But the rollout of the arbitration system has been plagued by lawsuits, shutdowns, and conflict over the fairness of awards.

The new data tracks with previous numbers for the first half of 2023 that CMS released in February, which illustrate that the law is not working as the Congressional Budget Office projected. CBO predicted the arbitration process would largely keep disputed bills closer to the in-network rate, which is what usually determines the cost-sharing for patients under their insurance plans.

The median awards in the third quarter of 2023 ranged from 100% of the median in-network rate for complex drug and biologic administrations to 1,075% of that rate for vascular diagnostics. Median arbitration awards for most service types fell between 200% to 600% of the median in-network rate, also known as the "qualified payment amount."

The same was true of arbitration disputes in the fourth quarter. Median awards ranged from 100% of the qualified payment amount for lab services to 1,262% for neurology services.

Christine Cooper, who represents health plans and enrollees in surprise billing disputes as CEO of aequum, said the new data were not unexpected.

"The big question is why is the 'win rate' so high for providers?" she said in an email.

The arbitration process is the subject of a litany of court battles over the Biden administration's implementation, enforcement of the awards, and alleged deception from the opposing party. Much of the litigation centers on the weight and accuracy of the qualified payment amount.

Jeffrey Davis, who works with providers as health policy director at McDermott+Consulting, argued the data show that independent arbitrators view the qualified payment amount as unreasonably low and not reflective of the market rate.

"The fact that the median prevailing offers as a percentage of the QPA are all over the map also demonstrates that the QPA is an unreliable number that is not a meaningful representation of an appropriate payment rate," he said in an email.

A number of providers have sued health plans over what they say are artificially low QPA offers after they lose in arbitration, but the courts are split on whether they have the right to bring those disputes to litigation.

IRS Plans More Nonprofit Hospital Audits as Scrutiny Heats Up

The IRS will audit dozens of tax-exempt hospitals this year, a top agency official said.

The exams come amid continued criticism of nonprofit hospitals, which some lawmakers say are abusing their tax-exempt status by not providing enough charity care.

The agency intends to open 35 examinations in fiscal year 2024, Robert Malone, director of exempt organizations and government entities at the IRS, said Friday during a panel at the TEGE Exempt Organization Council Exempt Organizations Update. Hospitals are required to show they provide "community benefit" to retain their tax-exempt status.

"This strategy is in the early stage, so we don't have emerging issues from these examinations yet," Malone said during the panel.

The agency has already "opened a number of examinations" into hospitals and provided formal training to revenue agents about the compliance issues, he said.

- Lawmakers last summer pressed the IRS and Treasury Department to increase scrutiny in this area. The Government Accountability Office said in a report last year that the IRS should update its Form 990 to allow hospitals to provide more detailed information about their community benefits.
- The IRS also did 2,700 compliance checks into tax-exempt organizations to make sure they're paying the 21% excise tax if they paid certain employees more than $1 million. About a quarter of those cases resulted in a tax change or penalty, Malone said.

Medicare Updates Star Ratings That Inform Insurers' Payments

The US government is updating crucial quality ratings for private Medicare plans, paving the way for 2025 bonus payments worth hundreds of millions of dollars to insurers that operate health plans for seniors.

The Centers for Medicare and Medicaid Services will recalculate the five-star quality rating system following specific guidelines outlined in a court decision, according to an emailed statement Friday. The updated ratings will determine bonus payments for Medicare Advantage plans for 2025.

The CMS announcement follows legal wins last week by health insurers SCAN Health Plan and Elevance Health Inc. against the Department of Health and Human Services. The insurers had filed suit against the agency, arguing that regulators used flawed methods to determine the ratings.

Medicare, the government health program for the elderly, uses the star system as a quality measure to help older Americans choose plans that do a better job of improving their health. Plans with higher ratings are given additional funding from CMS and can use that money to lower costs for beneficiaries, making their plans more appealing to customers.

Bonus payments can have a significant impact on a company's financial success. The changes from CMS provide insurers with a much-needed boost, as the Medicare Advantage business is already facing challenges such as increasing medical costs.

The news was first reported by the Wall Street Journal. Insurer shares were little changed in trading before US markets opened.

Lawmakers Take Aim at PE Health-Care Binge

Private equity's role in the health-care industry is a hot topic among US antitrust regulators—both federal regulators and state enforcers are focused on whether and how private equity ownership impacts quality and availability of care.

State and federal legislators are also taking note, introducing legislation aimed at curbing what some see as the risk of permitting the private equity business model to expand in the health-care industry.

A bill introduced this week in the US Senate, and one pending before the California senate, demonstrate the primary government concerns about ownership in health care. Regardless of the outcome of these specific bills, the private equity and hedge fund industries should be prepared for further pressure around investments in health care. The trend towards increased scrutiny of private equity's role in health care has legs.

Criminal Penalties

Senators Elizabeth Warren (D-Mass.) and Ed Markey (D-Mass.) introduced the "Corporate Crimes Against Health Care Act" on June 11. In simple terms, the bill makes it a felony for a person to contribute to the insolvency of a health-care entity if that insolvency leads to the "death or injury" of a patient under the care of that entity.

The bill also includes civil penalties, claw back provisions, and other penalties associated with specific insolvency measures for any health-care entity owned by a private fund. And those penalties attach to "any current or former director, officer, or control person of, or agent for, a private equity firm or target firm" and "any current or former shareholder" or active joint venture partner. In other words, the bill makes it illegal to permit a health-care facility owned by private equity to become insolvent and it "pierces the veil" when that happens.

The bill would allow the Justice Department and state attorneys general to claw back all compensation, including salaries, issued to private equity and portfolio company executives within a 10-year period before or after an acquired health-care firm experiences enumerated events of insolvency. A civil penalty of up to five times the claw back amount can be added. It changes the tax code in ways meant to make health-care acquisitions less attractive to private equity and would require health-care providers receiving federal

funding to publicly report mergers, acquisitions, changes in ownership and control, and financial data, including debt and debt-to-earnings ratios.

Angry Senators
In their announcement, Warren and Markey point to Cerberus Capital Management's purchase of Steward Health Care, which operated eight hospitals in Massachusetts, as the impetus for the bill.

The bill seeks to "prevent what happened with Steward from ever happening again," Warren said in the press release. "When private equity gets hold of health care systems, it is literally a matter of life and death, so if you drive a hospital like Steward into bankruptcy, putting patients and communities at risk, you should face real consequences."

Markey called Cerberus Capital's actions with regard to Steward-owned hospitals "unforgiveable."

Regardless of whether this bill can pass Congress—and it's unclear that much of anything will this year—that outrage is an important fact for market participants to gauge. If legislators feel strongly about what's happening in the industry, it's unlikely they'll let this issue drop. And the legislative climate could change as early as January.

California Concerns
A bill pending before the California senate also seeks to check both private equity acquisitions in the sector and private equity interjecting itself into the management of physicians' practices.

AB-3129, which passed the California house in May and now sits in committee in the senate, requires notice and consent from the state attorney general before a private equity or hedge fund can purchase a hospital or provider group in the state. That would mean private equity purchasers would be subject to the same notice and consent hurdles that currently apply to nonprofit hospitals in California seeking to reorganize or change control.

The bill also prohibits private equity or hedge fund owners of physician or psychiatric practices from controlling or directing that practice. It forbids California physicians or psychiatric practices from entering agreements (directly or indirectly) with private equity or hedge funds to provide management services to the practice for a fee.

The concern, expressed by California Attorney General Rob Bonta and 10 other attorneys general in a letter to federal regulators, is that the short-term horizon for profit taking in the private-equity industry isn't compatible with the values required in a health-care setting. A model that loads debt and management fees onto the purchased company, while demanding cost-cutting, negatively impacts patient care and outcomes.

Further, the attorneys general said, burgeoning consolidation leads to higher prices, lower-quality care, and reduced access to care for patients. They predict that the current wave of horizontal integration will soon be followed by a vertical wave that further restricts patient choice and outcomes without reducing cost.

The bill would place a block between California hospitals and further roll up through private equity. The last day for each house of the California legislature to pass bills is Aug. 31.

FTC, DOJ Investigate
The Federal Trade Commission, Justice Department, and Department of Health and Human Services jointly launched a cross-government public inquiry into private equity's and other corporations' increasing control

over health care in March. The agencies issued a request for information on consolidation in health care. The extended comment period ended June 5.

The agencies received over 6,000 comments.

Medicare Report to Congress Highlights Program Challenges, Goals

A new report from a congressional advisory panel offered good and bad news for Medicare managed care companies.

The Medicare Payment Advisory Commission's annual June report to Congress found that 95% of 37.5 million prior authorization requests by Medicare Advantage plans in 2021 had "fully favorable decisions." And 80% of negative prior authorization decisions that year also had "fully favorable decisions" upon redetermination.

The findings come as Congress and regulators heighten their scrutiny of care denials by MA plans.

"Prior authorization has been identified as a major source of provider administrative burden and can also be a health risk for patients if it results in needed care being delayed or denied," Paul Masi, MedPAC's executive director, said during a press briefing Thursday.

But the report also found "important shortcomings" remain in the data on patient-provider encounters that MA plans submit to the Centers for Medicare & Medicaid Services. That data "is not internally consistent," Masi said. The report also found "important discrepancies suggesting that encounter data remained incomplete, particularly for some organizations," Masi added.

"Complete and accurate encounter data could be used to provide more rigorous oversight of Medicare's payments to MA plans—which reached $455 billion in 2023," a commission press release said.

The commission's annual June report looks at improvements to Medicare payment systems, changes to health-care delivery, and other issues affecting Medicare.

The commission threw its support to a proposal to update clinician payment and incentivize participation in Medicare alternative payment models. The commission "will continue to develop this option in the future," the press release said.

The report also looked at challenges faced by hospitals that participate in Medicare's Acute Hospital Care at Home (AHCAH) program, which provides hospital care in a beneficiary's home. By April, about 23,000 Medicare and Medicaid beneficiaries had been discharged from the program. But the commission said some of the 328 hospitals approved for the program didn't implement programs.

Interviews with hospital staff found some beneficiaries wouldn't participate in the program due to unfamiliarity with it. The program may also cost more than traditional hospital stays "due to the additional costs and inefficiencies of providing care to patients in their homes," the release said.

Further study is needed to see if the program can provide better outcomes and reduced spending for follow-up care, the commission reported.

UnitedHealth Hack Fuels Bids to Shield Americans' Medical Data

Cyberattacks compromising the health information of millions of Americans are prompting Congress and the Biden administration to take action to better protect highly sensitive personal data that's profitable for hackers.

Up to a third of Americans had their private health information exposed in the cyberattack on Change Healthcare in recent months. The breach is believed to be the largest in health care in US history and has cost parent company UnitedHealth Group Inc. up to $1.6 billion in profits this year.

Lawmakers and regulators have been scrambling in their response. In May, Senate lawmakers grilled UnitedHealth Group CEO Andrew Witty over the attack, pressing the embattled executive on why the company left so much health information vulnerable and what should be done to avoid a repeat. Shortly after, the White House said it was weighing standards for hospitals to better protect patient information.

Now, senators on both sides of the aisle are keeping an open line with Witty and weighing legislation to better protect health information. They've also upped the pressure on the Biden administration's labor and health departments to take on a greater role in both preventing and responding to cyberattacks.

The Department of Labor didn't immediately respond to a request for comment. However, a Health and Human Services Department spokesperson said the agency is considering issuing new enforceable cybersecurity standards for the health-care sector, a move that could face a backlash from hospitals.

Trade group American Hospital Association has been vocal in its opposition to mandatory cybersecurity requirements for hospitals. In a May interview, the AHA's national adviser for cybersecurity and risk, John Riggi, said that should the government take regulatory action, "hospitals alone should not be singled out."

"The government needs to do more on offense against the fundamental source of cyber risk, foreign hackers and ransomware gangs attacking health care, " Riggi said. "That's not hospitals' job. That's the US government's job."

Lawmaker Response

The FBI said in a report that in 2023, the health-care and public health sector flagged the most ransomware attacks, with organizations having filed almost 250 complaints with the agency. That's more than critical manufacturing, which flagged fewer than 220, and government facilities, the third-most hit sector in the report, which came in at 156.

The full extent of Change's breach has yet to be determined. The company processes pharmacy requests and insurance claims for over 340,000 physicians and 60,000 pharmacies. The hack was discovered Feb. 21, and the company severed connections that distribute data and money across the health-care system, leading to a backlog of payments and claims.

Lawmakers are casting a wide net in their response. Some, like senators Ron Wyden (D-Ore.), who chairs the Senate Finance Committee before which Witty testified, and Bill Cassidy (R-La.), a member of that committee, are pushing for legislation to better protect critical health-care infrastructure.

Wyden said he's working on proposing "minimum standards" for cybersecurity in health care. He said the details wouldn't be revealed until later as part of legislation.

Wyden also called for the Federal Trade Commission and the Securities and Exchange Commission to investigate UnitedHealth to determine if laws were broken, Bloomberg News reported.

Cassidy said there's two tracks for responding to Change: looking at what happened at the company, as well as examining the broader health industry.

Witty, Cassidy said, has remained available since the hearing to answer questions. Cassidy said one issue that's been brought to his attention is that UnitedHealth was unable to do a full security analysis of Change before purchasing the company.

Cassidy said he is also concerned there are too many larger companies operating in the health-care space. "Should we have any organization that, if it goes down, everything else is affected?" he asked.

While he isn't currently putting forth legislation, Cassidy said Congress should act. The lawmaker, who also is the top Republican on the Senate Health, Education, Labor and Pensions Committee, said if he becomes HELP chairman in the next Senate, cyber "will be a big priority."

"It's better that Congress take information from all stakeholders—as opposed to what inevitably is a narrower view of a particular administration," Cassidy said.

Agency Activity
The Biden administration is facing increasing pressure to take direct action on cyber safety.

Earlier this month, House Committee on Education and the Workforce Chairwoman Virginia Foxx (R-N.C.) wrote to the Department of Labor to ask what the Employee Benefits Security Administration is doing to investigate cyberattacks.

Foxx's committee's jurisdiction includes private employer health-care benefits. She wrote the committee is concerned about how the Employee Benefits Security Administration "is working to curb" risks for employer-sponsored benefit plans.

Her letter included a list of questions about the EBSA's cybersecurity role, such as how many cybersecurity investigations the group has conducted since February 2021 and whether the agency has ever been "compromised by cybercriminals." Foxx asked for responses by May 30.

"The Change Healthcare hack immediately affected workers' and their families' access to health care. Prescriptions could not be filled. Health care claims and payments were halted. Pharmacies, military hospitals, and clinics attempted workarounds to mitigate disruptions," Foxx wrote.

In a March statement, the HHS said it was in regular contact with UnitedHealth leadership and others to ensure the effectiveness of the company's response.

Days later, the HHS and DOL published a letter to health care leaders saying the agencies urge UnitedHealth, insurance companies, and other payers to take actions, though they stopped short of enforcement.

The HHS in May said that hospitals can require UnitedHealth notify patients if their data was compromised in the February attack.

The department is considering enforceable actions informed by voluntary performance goals for health sector groups released in January, according to an agency spokesperson.

Among those goals are things like reducing email security risks, adding multifactor authentication, and setting security requirements for outside vendors.

The HHS spokesperson declined to provide additional information on enforcement specifics, including who in the agency would be responsible.

Enforcement

Greg Garcia, executive director for cybersecurity of the Health Sector Coordinating Council, an advisory group that works with the government, said enforcement is "a difficult thing to do," but would make a difference in improving health sector cybersecurity.

Garcia said a federal rule —which implements standards under the Health Insurance Portability and Accountability Act—currently requires health providers to have incident response plans, and that it's enforced by the HHS Office for Civil Rights. In the event of cyber incidents, the HHS "depends on intel from industry, law enforcement," and others, Garcia said, though "the interagency process and its information sharing protocols with industry are always a work in progress."

An HHS spokesperson noted that the civil rights office investigates complaints filed with the group and conducts compliance reviews. Investigations may result in civil fines. The spokesperson also said the office submitted requests for Congress to increase the amount of fines it can impose in a calendar year, with the goal being to promote HIPAA compliance to protect sensitive patient data.

Still, Garcia noted the Change attack was due to problems with "basic cyber hygiene"—a lack of multifactor authentication—and that "no amount of cyber security controls will totally prevent cyberattacks."

Cybersecurity is a "collective responsibility" that health providers can't shoulder alone and the government does have a role to play, said Garcia, who has worked with the HHS on cybersecurity matters. Congress could help by giving the HHS and other agencies broad authority to fund or oversee better incentives for the private sector, he said.

He added that third party service providers are also responsible. "Change Healthcare is a third party service provider, and they screwed up and the fallout impacts their customers existentially," Garcia said.

Under its 2025 fiscal year budget request, the HHS would create a $1.3 billion Medicare incentive program for encouraging hospitals to take up cybersecurity practices. The department noted there was a 95% increase in large breaches reported to the agency from 2018 to 2022.

The AHA's Riggi said any minimum standard placed on hospitals alone wouldn't solve health-care sector cybersecurity risks. Focusing solely on hospitals wouldn't have prevented the Change attack, Riggi said.

"We need to secure the entire health-care system," he said.

Medicaid Fraud Singled Out as Program Costs Approach $1 Trillion

Washington policymakers are stepping in to stem a tide of fraudulent and improper payments being made through Medicaid, which analysts say could threaten the long-term solvency of the nation's largest health insurer.

About $50.3 billion—or 8.6% of all Medicaid payments—were made improperly last year. The Government Accountability Office estimates the Medicaid program accounted for nearly 21% of all government-wide improper payments.

Medicaid provides health coverage for approximately 76 million low-income individuals. With nationwide spending on the program projected to surpass $1 trillion by 2032, lawmakers from across the political spectrum have pushed the Biden administration to address holes in oversight and accountability.

Improper payments occur when payments fail to meet program requirements due to unintentional errors, insufficient documentation, or fraud, and can include both overpayments and underpayments.

Last October, House Energy and Commerce Committee leaders pressed the Centers for Medicare & Medicaid Services on why significant Medicaid payments were being made to beneficiaries who had passed away. Around the same time, the Department of Health and Human Services' Office of Inspector General identified over $249 million in payments made to Medicaid managed care plans on behalf of deceased enrollees.

The lawmakers also noted that states frequently covered beneficiaries who are enrolled in two states at the same time and that the CMS lacked a standardized method to review the screening and eligibility processes used by providers.

Now, lawmakers including Reps. Gus Bilirakis (R-Fla.), Angie Craig (D-Minn.), Mike Garcia (R-Calif.), and Mariannette Miller-Meeks (R-Iowa) have introduced a series of bills that would force the CMS to address these vulnerabilities head on.

The legislation includes measures to verify beneficiaries' eligibility quarterly and ensure they are alive (H.R. 8084), screen out medical providers who have died (H.R. 8089) or have been terminated from Medicaid (H.R. 8112), and confirm beneficiaries are not enrolled in multiple states (H.R. 8111). All four bills advanced unanimously during a Wednesday markup by the House Energy and Commerce Committee.

Bilirakis emphasized the urgency of passing these bills, saying they are part of the solution to safeguard the viability of the Medicaid program. "I think people realize that we need these dollars for the truly sick," he said in an interview.

Congressional Action

The four bills are aimed at reducing improper Medicaid payments by requiring states to modernize their information systems. Despite potential long-term savings, lawmakers told Bloomberg Law that some states have been reluctant to update their legacy systems due to the associated costs.

"Sometimes in government there's inertia, and it takes the prodding of another government entity that makes laws to prod individuals into doing something that makes sense to do," Miller-Meeks said.

Her bill, the Medicaid Program Improvement Act (H.R. 8111), focuses on ensuring the reliability of address information so that state Medicaid programs don't pay for beneficiaries enrolled in two states. A 2022 OIG

report identified 327,497 beneficiaries enrolled in two states, costing state Medicaid programs over $117.1 million in double payments in August 2020.

Beginning in 2026, the measure would require states to regularly obtain enrollee address information from reliable data sources and promptly act on any address changes. Medicaid managed care organizations would also be required to transmit address information provided directly by enrollees to the state.

The Leveraging Integrity and Verification of Eligibility for Beneficiaries Act (H.R. 8084), sponsored by Bilirakis and Craig, would require states to review the Social Security Administration's death master file every quarter to identify and disenroll deceased individuals from their Medicaid rolls. States would also be required to discontinue Medicaid payments made on behalf of deceased enrollees.

Two bills—H.R. 8112 sponsored by Rep. Anthony D'Esposito (R-N.Y.), and H.R. 8089, sponsored by Garcia and Rep. Scott Peters (D-Calif.)—contain provisions to strengthen Medicaid provider screening. The bills would mandate that beginning in 2025, states check a federal database during provider enrollment and revalidation to determine if the provider has been terminated from Medicare, Medicaid, or CHIP in any state.

H.R. 8089 would also require quarterly checks of the death master file to identify deceased providers. This provision would allow states to confirm that doctors are not dead before being automatically re-enrolled in Medicaid, Peters said during the Energy and Commerce markup.

Additional Steps

Drew Gonshorowski, a senior research fellow at the Paragon Health Institute, said the bills are a step in the right direction, but they don't address one of the largest sources of improper payments in the Medicaid program—undercount.

"We have to be careful with improper payment reports because they're not necessarily a full picture of the problem, because during Covid, for example, CMS didn't do eligibility checks," Gonshorowski said.

"So, you're actually undercounting the nature of the size of these improper payments," he said.

A recent Health Affairs study estimated that nearly half of the 5.9 million people projected to lose coverage after the expiration of the Covid-19 public health emergency's continuous coverage provision had already reported being uninsured.

According to Gonshorowski, a plurality of the surveyed beneficiaries could have been enrolled in both Medicaid and private insurance. "All of it is money directly to insurers' pockets," he said.

The April GAO report on the scope of improper payments across Medicare and Medicaid also identified areas of concern that Washington policymakers have yet to substantially address with administrative action or legislation.

These included recommendations that Congress require states to report information on the sources of funds used to finance the non-federal share of supplemental payments, which the GAO says often results in surplus Medicaid payments that may not align with patient volume or costs.

For example, in February 2016, the GAO reported that nine hospitals that obtained large supplemental payments received average surplus payments of about $39 million, and used those revenues "to fund hospital operations, maintenance, and capital purchases, such as a helicopter."

The GAO also identified concerns over increased spending on Medicaid demonstrations, which allow states to test new coverage and service delivery options as long as the demonstration is budget-neutral. Since 2008, the agency has asked Congress to consider establishing new statutory requirements for the HHS to more clearly outline the methods used to demonstrate budget neutrality.

Biden Moves to Bar Medical Debt From Consumer Credit Reports

President Joe Biden's administration formally proposed a rule to bar medical debt from most individual credit reports on Tuesday, a move that will prevent major health care bills from negatively impacting borrowing.

Vice President Kamala Harris and Consumer Financial Protection Bureau Director Rohit Chopra announced the measure, which is expected to affect more than 15 million Americans, according to a White House fact sheet.

The administration estimates that beneficiaries could see their credit scores raised by an average of 20 points if the changes are enacted, and approximately 22,000 more mortgages could be approved each year.

The move is the latest effort from the administration to help lower costs for consumers ahead of November's election rematch between Biden and Republican Donald Trump, in which inflation will be a key issue.

"No one should be denied access to economic opportunities simply because they experienced a medical emergency," Harris told reporters on Tuesday, calling on states and local governments to take similar actions to reduce medical debt burdens.

The proposed rule will enter a public-comment period until Aug. 12. It would not take effect until early next year, likely placing it on the chopping block if Biden fails to win reelection. Republicans have been critical of debt-related policy actions under Biden, in particular his efforts to relieve student-loan debt for millions of borrowers.

The proposal has been percolating for months. The CFPB said last year it was working on the change. At the time, the agency was also looking to stop lenders from considering such debts when borrowers sought loans or other credit and curb certain repayment practices.

Three major credit-reporting agencies — TransUnion, Equifax Inc. and Experian Plc — have already voluntarily removed certain existing medical debt from credit reports.

Nonetheless, a CFPB report released in April found that medical bills appeared on the credit reports of 15 million Americans despite changes by those agencies, with more than $49 billion in outstanding medical debt in collections.

Medicaid Advisers Urge Enhanced Transparency, Care Coordination

Advisers to Congress on Medicaid policy recommended on Tuesday measures to enhance the transparency of the program's financing and improve care coordination for beneficiaries eligible for both Medicaid and Medicare.

In its June report to Congress, the Medicaid and CHIP Payment and Access Commission also made recommendations to optimize state Medicaid agency contracts, analyzed enrollment trends in Medicare Savings Programs, and emphasized the need for better demographic data collection.

The report follows MACPAC's annual March report, which focused on improving beneficiary stakeholder engagement, rectifying funding cuts to safety-net hospitals, and streamlining the appeals process for beneficiaries denied claims by Medicaid-contracted insurers.

In the new report, MACPAC recommends that Congress amend the Medicaid statute to require states to submit annual, comprehensive reports on their Medicaid financing methods and the amounts of the non-federal share of Medicaid spending acquired from all providers, not just hospitals and nursing facilities. The report said this increased transparency will enable policymakers to analyze the full scope of net Medicaid payments and provide a clearer understanding of how providers are paid under alternative financing mechanisms.

The report also emphasizes the importance of coordinating care for individuals who are dually eligible for Medicaid and Medicare. According to MACPAC, dually eligible beneficiaries can experience fragmented care and poor health outcomes when states don't do enough to synchronize Medicare and Medicaid benefits.

The June report recommends states require Medicare Advantage dual-eligible special needs plans to regularly report data on care coordination and utilization. The commission also calls on the Centers for Medicare & Medicaid Services to issue guidance supporting states in developing integration strategies tailored to their specific health-care landscapes and populations.

Additionally, the report examines enrollment trends in Medicare Savings Programs, which uses Medicaid funding to subsidize Medicare premiums for low-income seniors. It finds enrollment has increased across all MSP categories from 2010 to 2021, with approximately 80% of dually eligible beneficiaries enrolled in an MSP in 2021.

MACPAC's report also highlighted the need for improved demographic data collection in Medicaid to better measure and address health disparities among historically marginalized populations. The commission encourages the CMS, states, researchers, and other stakeholders to capitalize on existing English proficiency, sexual orientation and gender identity, and disability data to help measure and address health disparities.

LEGAL

HHS Asks Court to Deny Florida Bid to Block Transgender Care

The Biden administration is urging a federal judge to shoot down Florida's request to block a federal transgender health civil rights rule from going into effect, arguing the state is incorrectly framing its requirements.

Florida's bid to stop a Department of Health and Human Services rule prohibiting health discrimination for someone's gender identity is "premised on several misapprehensions," the government said Thursday. The state wants the US District Court for the Middle District of Florida to block the rule from going into effect in July, a move the HHS said is outweighed by "the public interest" and "potential harms" to others.

The dispute comes ahead of a June 21 hearing on Florida's request for the court to stay the HHS rule. Released earlier this year, the rule involves the hotly contested Section 1557 of the Affordable Care Act, which has drawn at least three other lawsuits in recent weeks from states and a children's clinic.

Florida and the Catholic Medical Association filed their challenge in May, claiming the rule forces doctors to perform gender-affirming surgeries while requiring insurance issuers and states to "subsidize gender transitions."

The HHS pushed back. In Thursday's filing, the agency said "nothing in the Rule requires the provision of or insurance coverage for any particular health service where the covered entity has a legitimate, nondiscriminatory reason for denying or limiting the service or coverage."

The HHS also said the rule repeatedly makes clear that Section 1557 "does not apply insofar as any nondiscrimination obligation it creates would violate applicable Federal protections for religious freedom and conscience, including the Religious Freedom Restoration Act."

"The Rule provides that discrimination on the basis of gender identity is prohibited sex discrimination under" Section 1557, the HHS said. "Plaintiffs' arguments to the contrary ignore the statutory language and are rooted in hypothetical future disagreements with HHS about possible applications of the Rule that do not reflect anything in the Rule itself."

The case is Florida v. HHS, M.D. Fla., No. 8:24-cv-01080, response filed 6/13/24.

Tempus AI Copied Guardant Patents to Create Tests, Lawsuit Says

Tempus AI Inc. infringed five Guardant Health Inc. patents to create copy-cat diagnostic DNA tests, according to a new federal lawsuit.

The market success of Tempus's tests derives from its unauthorized use of Guardant's "groundbreaking" cancer diagnostics patents, Guardant said Tuesday in a complaint filed in the US District Court for the District of Delaware.

Tempus filed for an initial public offering on May 20 and noted that it could be subject to claims of patent infringement, mentioning other litigation involving Guardant in its S-1 filing with the US Securities and Exchange Commission. Tempus also said in the filing it's possible the company would need to modify existing or future sequencing methods or license intellectual property from third parties, "both of which could be time consuming and expensive."

The company, which uses artificial intelligence to process medical data, didn't immediately respond to Bloomberg Law's request for comment.

Guardant is a "leading" precision oncology company, the complaint said, and it develops blood tests to screen patients for multiple cancers and diseases at once. Such tests are faster and less painful and expensive than invasive biopsies, according to the complaint. It offers seven tests, including Guardant360® CDx, which was the first FDA-approved liquid biopsy test.

Guardant's years-long investment and extensive research resulted in "cutting-edge" innovations covered by more than 95 US patents, it said. Tempus allegedly infringed US Patent Nos. 11,149,306, 9,902,992, 10,501,810, 10,793,916, and 11,643,693.

Each accused test "practices steps that are identical or equivalent" to Guardant's inventions, the complaint said.

Guardant seeks an injunction against Tempus, damages, and mandatory future royalty payments, among other relief.

Potter Anderson & Corroon LLP and Wilson Sonsini Goodrich & Rosati represent Guardant.

The case is Guardant Health Inc. v. Tempus AI Inc., D. Del., No. 24-cv-00687, 6/11/24.

Court Split Spells Trouble on Surprise Billing Award Enforcement

A continued fight between medical providers and insurance companies over how to enforce arbitration awards in surprise billing disputes is splitting the courts and bringing greater uncertainty to an already complicated and fraught process.

Judge Jane Boyle of the US District Court for the Northern District of Texas recently dismissed a suit from air ambulance providers Guardian Flight LLC and Med-Trans Corp. that sought to force insurer Health Care Service Corp. to pay money they were awarded through No Surprises Act arbitration, finding that the law provides no right to sue in court.

By contrast, Judge Kevin McNulty of the US District Court for the District of New Jersey did enforce an arbitration award last September, denying physician practice GPS of New Jersey M.D. P.C.'s request to overturn the final amount owed by Horizon Blue Cross Blue Shield of New Jersey.

Attorneys and lobbyists for providers fear the potential lack of an enforcement mechanism could unravel the already tortured NSA arbitration process, where providers, plans, and arbitrators are entangled in battles over allegations of delayed or nonpayments for services, errors, and misrepresentations.

The No Surprises Act, enacted in 2021 as part of a government funding measure, was intended to shield patients from unexpected out-of-network bills in the event of an emergency or certain instances where they reasonably expected to be receiving in-network care.

Medical providers and health plans are directed under the NSA to work out any related billing disputes through arbitration.

But it has been difficult at times for parties to even use the system because of a shutdown following litigation challenging its setup, conflicts over dispute eligibility, and a case volume that in the first half of 2023 alone reached 13 times the number of disputes federal agencies had predicted for a full calendar year.

HHS, Not Courts

Insurance companies have argued that providers are unfairly trying to force payment in arbitration on disputed claims that contain critical errors like mistakes in contact information and inaccuracies in eligibility determinations. Aetna Inc., for example, said in one case that some awards cited by a provider in their suit didn't even involve the insurer.

Adam Schramek, a partner at Norton Rose Fulbright who represented the providers in the Texas lawsuit, said the NSA's language makes arbitration decisions binding on both plans and insurers.

"The courthouse door should be open for them to enforce those obligations," said Schramek, who's also representing air ambulances in another federal case against Aetna Health Inc. and other insurers over delayed payments.

Insurers argue instead that the Department of Health and Human Services is the proper place to adjudicate complaints, although the Centers for Medicare and Medicaid Services—the HHS subagency charged with handling such matters—is already bogged down by arbitration cases.

"HHS accepts provider complaints—including complaints that health plans are not timely paying [independent dispute resolution] IDR awards—and performs complaint-based audits to enforce the NSA's provisions," HCSC wrote in its motion to dismiss the Texas suit.

CMS has said the agency is "actively investigating and addressing complaints."

In the case against Aetna Health, the insurer argued that it's willing to pay out claims through arbitration once verified, but objected to providers' requests for attorneys' fees, costs, and pre-and post-judgment interest.

Providers Prevail

Insurance companies aren't faring as well as the Congressional Budget Office and others predicted.

Preliminary data shows that providers are winning the majority of arbitration disputes, according to an analysis from the Brookings Institution, while the Commonwealth Fund found that a handful of private-equity backed companies are the main drivers behind the arbitrations.

Yet despite the high win-rate for providers, a 2023 survey of physicians found that insurers weren't paying 52% of arbitration awards.

Several lawyers said they expect the Texas decision to be overturned on appeal, considering that the result—the inability to enforce arbitration awards—would upend the process that Congress created.

"The system just isn't going to work if the provider can't force the plan to pay," said Roberta Casper Watson, a partner at the Wagner Law Group who works with employers on health benefits.

Commercial claims data revealed by CMS in February show that insurance companies are often paying typical out-of-network rates, undermining predictions from the CBO that payment rates would trend toward in-network amounts.

Analysts fear the trend could raise insurance premiums and in-network prices if it continues.

Federal Arbitration Act

Michael Gottlieb, a partner at Gottlieb and Greenspan LLC, said one notable distinction between the Texas and New Jersey cases is reliance on the Federal Arbitration Act, which governs the enforcement of arbitration awards generally.

The FAA helped form the linchpin in McNulty's decision to confirm the awards in the New Jersey case, said Gottlieb, who represented the physician practice.

"The judge ruled that the Federal Arbitration Act, coupled with the No Surprises Act, allows the court to confirm the award," he said.

But the NSA itself contains no provision enforcing the awards, said aequum LLC CEO Christine Cooper, who represents small, self-funded health plans in the arbitration process and in court.

The Texas judge's decision was correct, as Congress chose to incorporate other provisions of the FAA into the NSA, she said.

"The fact that the legislature incorporated some of the FAA and not all of the FAA kind of eliminates or attacks that implied-rights type argument," she said. "Because they could have included the whole thing. They could have included at least the enforcement mechanism, and they didn't."

It would be "most appropriate" for Congress itself to revisit these issues, she said.

Schramek said that while he believes the awards are enforceable under the NSA, the Texas judge's ruling that amending the case would be futile implied she would reject an FAA claim as well.

"I think at the end of the day, the judge in Dallas just reached a different conclusion from the judge in New Jersey," he said.

It's hard to say how the question of court enforcement will be resolved, said David Greenberg, a partner at ArentFox Schiff LLP.

"I think that it depends on which jurisdictions and which judges get these cases," he said. "This is pretty early on."

Neither the attorneys for Horizon at Stradley Ronon Stevens & Young or for HCSC at Reed Smith responded to a request for comment.

New Opportunities

Some insurance companies also are recalculating patient cost sharing amounts after losing arbitration disputes, said Jeffrey Davis, health policy director at McDermott+Consulting who works with providers.

He pointed to a letter the Emergency Department of Practice Management Association and the American College of Emergency Physicians wrote to the departments of Health and Human Services, Labor, and Treasury in February, which contained examples of health plans doing just that.

That's a direct violation of the NSA, he said. If the courts aren't willing to enforce the awards, patients could end up getting billed more again.

"I think this is setting up a dangerous precedent," Davis said of the Texas decision.

Other recent lawsuits could give the courts more opportunities to flesh out whether and how NSA arbitration awards will be enforced.

GPS has sued to force Aetna Life Insurance Co. to pay the remainder of an arbitration award for treating an emergency patient, citing both the NSA and FAA.

Air ambulance company Air Methods LLC sued Independence Blue Cross LLC, bringing claims under the FAA and NSA. They also cited a section of the Employee Retirement Income Security Act that allows beneficiaries to sue when they believe they have been wrongly denied benefits.

Air Methods says it has ERISA standing because it "steps into the shoes of" enrollees in Independence's self-funded plans and payments and benefits are assigned to the provider under the plan.

But Judge Boyle rejected a similar ERISA argument in the Guardian Flight case, noting that enrollees are theoretically protected from surprise bills under the NSA, and are therefore not harmed.

Neither Aetna nor Independence has yet filed a response to the complaints.

High Court Agrees to Revisit 2022 Medicare Payment Ruling

The US Supreme Court announced Monday it will accept a case that asks for greater clarity on the justices' 2022 ruling that upheld the way Medicare calculates payments for certain hospitals.

The case, Advocate Christ Medical Center v. Becerra, revolves around the meaning of the phrase "entitled to benefits" and it involves two separate lawsuits.

In Becerra v. Empire Health Foundation, the high court in June 2022 upheld a 2005 rule that decreased the amount of extra Medicare payments hospitals receive for serving a larger share of poor patients. The decision meant some providers might not be able to recoup the higher costs they say they spend treating low-income patients. In the decision, the justices agreed with the Department of Health Human Services that "individuals 'entitled to [Medicare Part A] benefits' are all those qualifying for the program, regardless of whether they are receiving Medicare payments for part or all of a hospital stay."

The Medicare statute maps out how the HHS should calculate these annual supplemental payments, known as disproportionate share hospital (DSH) adjustments.

But in July 2017, Advocate Christ Medical Center in Oak Lawn, Ill., and more than 200 hospitals, had already sued the HHS over the department's method of determining DSH payments. The hospitals claimed the formula didn't fully account for care provided to patients eligible for Supplemental Security Income benefits, which is used by the HHS as a proxy for care provided to low-income patients.

But the US District Court for the District of Columbia rejected the hospitals' arguments and granted summary judgment to the HHS in a June 2022 ruling that the disputed funding formula was consistent with the statute and reasonable. The court also denied the hospitals' claim for recalculation of their compensation for fiscal years 2006-2009.

Question Left Open

In December 2023, attorneys for the unsuccessful plaintiff hospitals petitioned the US Supreme Court to revisit its June 2022 decision in Becerra v. Empire Health Foundation.

They claimed the decision "expressly left open the question of whether 'entitled to [SSI] benefits' likewise includes all those who qualify for the SSI program," said the plaintiff's petition to the high court. The federal SSI program provides monthly payments to low-income people with limited resources, including disabled children, disabled adults, and people 65 years and older.

While the HHS "insists, contrary to its Medicare interpretation, that only patients who received an SSI cash payment for the month of their hospital stay are 'entitled to benefits.' This case thus presents Empire's open question: Does the phrase 'entitled to benefits,' used twice in the same sentence of the Medicare Act, mean the same thing for Medicare Part A and SSI, such that it includes all who meet basic program eligibility criteria, whether or not benefits are actually received," the petition asked of the high court.

"The Court should seize this opportunity to review this question of pressing importance, which affects the survival of safety net hospitals across the country and the health of the Nation's most vulnerable communities," the petition declares.

In a brief opposing the petition request, Justice Department attorneys argued "there is no circuit conflict for which this Court's review might arguably be warranted." They said petitioners "appear to assume—incorrectly—that the D.C. Circuit's decision will govern all hospital DSH payments nationwide."

"But the D.C. Circuit's decision constitutes binding precedent only in cases in which a hospital chooses to seek judicial review of its DSH payment (as part of its annual payment from the Medicare Program) in the District Court for the District of Columbia," the government brief said. "A hospital also has the option to seek review "in the district court for the judicial district in which the [hospital] is located."

Counsel for the petitioning hospitals include: Daniel F. Miller, Sara J. MacCarthy, Heather D. Mogden, of Hall, Render, Killian, Heath & Lyman; and Hyland Hunt and Ruthanne M. Deutsch, of Deutsch Hunt PLLC.

The case is Advocate Christ Med. Ctr. v. Becerra, U.S., No. 23-715, petition granted 6/10/24.

AROUND THE STATES

New York

Former Opioid User Revives Disability Bias Suit Against Hospital

A Glens Falls, NY, hospital will face claims that it discriminated against a pregnant recovering substance abuser based on her disability, a federal appeals court said.

Nicole Costin plausibly alleged that, during labor and delivery, Glens Falls Hospital violated the federal Americans with Disabilities and Rehabilitation Acts when it tested her for illicit drugs without her consent and reported her to state child protection authorities even though the test results were negative, the US Court of Appeals for the Second Circuit said Wednesday.

The court partially vacated the lower court's dismissal of the complaint, which was based on a finding that Costin hadn't adequately pleaded discrimination based on her disability.

Costin alleged that the hospital has a blanket policy of calling child protective services to report pregnant patients who are taking a drug used when treating an opioid addiction, the Second Circuit said. That allegation supported an inference that Glens Falls instigated an investigation against Costin based solely on her history of substance abuse, Judge Dennis Jacobs said.

The hospital couldn't succeed at this stage of the case on its affirmative defense that it's a mandatory reporter under the federal Child Abuse Prevention and Treatment Act, Jacobs said. The law requires hospitals to notify child protective services when a baby is born with and shown to be affected by substance abuse or withdrawal symptoms, he said. It isn't clear yet whether Glens Falls had a statutory duty to report here, he said.

Costin's drug-testing claim presented a closer question, the court said. Her allegation that Glens Falls has a blanket policy of testing all Subutex users didn't in itself support an inference of bias, it said. But Costin also alleged that the policy was based on a discriminatory motive—to determine if Subutex users were illegally selling their pills, it said. This raised an inference that hospital officials took "a pejorative view" of these patients as dishonest or drug dealers, the court said.

The court refused to revive Costin's claims that the hospital discriminated against her by denying her an epidural, accelerating her labor, refusing to discharge her baby, and failing to explain treatment alternatives. These actions clearly constituted medical decisions, it said.

Chief Judge Debra Ann Livingston and Judge Raymond J. Lohier Jr. joined.

Schulte Roth & Zabel LLP represents Costin. McPhillips, Fitzgerald & Cullum LLP represents the hospital. Martin Clearwater & Bell LLP and Rebar Kelly represented individual provider defendants. The US Justice Department filed an amicus brief supporting Costin.

The case is Costin v. Glens Falls Hosp., 2024 BL 201004, 2d Cir., No. 23-379, 6/12/24.

North Carolina

FTC Loses Bid to Block Novant Health $320 Million Hospital Deal

The Federal Trade Commission failed to block Novant Health Inc. from pursuing a $320 million deal to buy two North Carolina hospitals after a federal judge said the deal can move forward.

Novant's purchase of the Lake Norman Regional Medical Center and Davis Regional Medical Center from Community Health Systems is likely to promote added competition with other hospitals in North Carolina, Judge Kenneth Bell of the US District Court for the Western District of North Carolina said in a Wednesday order.

"The proposed merger carries at least as much likelihood of competitive benefits as it does competitive harm and the FTC is unlikely to ultimately be successful in proving that the transaction may 'substantially lessen competition,'" Bell said.

The ruling hands a win to Winston-Salem based Novant, which signed a $320 million agreement last year to acquire both hospitals. The FTC alleged the acquisitions would likely raise heath-care costs by several million dollars annually and diminish the quality of patient care.

Bell said the public's interest is "best served by Novant being permitted to own and operate LNR and Davis, pending the conclusion of the FTC administrative process."

The FTC declined to comment.

The case is Federal Trade Commission v. Novant Health, Inc., W.D.N.C., No. 5:24-cv-00028, 6/5/24.