# FEDERAL HEALTHCARE LAW UPDATE

## FEDERAL UPDATE

### Department of Justice Launches Antitrust Investigation of United Health

The United States Department of Justice (DOJ) recently opened an antitrust investigation into health insurance giant UnitedHealth. In particular, the DOJ is investigating the relationship between UnitedHealth and its Optum subsidiary. Optum has purchased numerous physician practices and now includes about 90,000 physicians, and other healthcare providers including surgery centers. The investigation comes as the Biden administration has stepped up antitrust enforcement in general, and has prioritized healthcare in its enforcement activity. The investigation presently is considered "non-public" and the DOJ has declined to comment on it. However, media sources discovered the investigation through a leaked email that a UnitedHealth executive sent to colleagues, advising that the DOJ had issued a sweeping notice to preserve documents related to the investigation.

The media sources advise that the DOJ investigators have been interviewing healthcare industry representatives in sectors where UnitedHealth competes. During the interviews, the DOJ has expressed concern about the possible anti-competitive effects of the relationship between UnitedHealth and Optum. Investigators have explored whether Optum's ownership of providers could present challenges to other health insurers that compete with UnitedHealth. Investigators also expressed concern whether UnitedHealth has favored Optum-owned physician groups through its contracting practices, to exclude rival groups from attractive payment arrangements. Further, investigators have asked whether the affiliation between UnitedHealth and the Optum-owned medical groups may result in violation of federal rules capping the amount a health insurer may retain from the premiums it collects. The DOJ also is investigating whether Optum excessively documents patients' health conditions, in an effort to increase Medicare payments for UnitedHealth's benefit. The UnitedHealth executive stated that despite these concerns, as yet the DOJ has issued no "specific allegations of wrongdoing."

***For more information, contact:***

**Isabelle Bibet-Kalinyak, Vice Chair** | 973.403.3131 | ibibetkalinyak@bracheichler.com

**Richard Robins** | 973.447.9663 | rrobins@bracheichler.com

### Physician Charged with $20.7M Health Care Fraud and Kickback Scheme

In February 2024, a federal grand jury in New Jersey returned an indictment charging a medical doctor with engaging in a health care fraud and illegal kickback scheme involving the submission of $20.7 million in false and fraudulent claims to Medicare for laboratory tests. According to the indictment, the physician allegedly received cash kickbacks from a laboratory representative and others in exchange for approving orders for laboratory tests billed to Medicare. As part of the scheme, the physician also allegedly participated in COVID-19 testing events at which he authorized COVID-19 tests as well as expensive and medically unnecessary cancer genetic tests that patients did not request, that were not used in the patient's treatment, and for which the patients rarely received the results. The indictment also charges the physician with participating in an illegal referral

scheme in which the physician solicited and received cash kickbacks and bribes from the owner of a medical equipment supply company in exchange for ordering orthotic braces that were not medically necessary.

The physician is charged with one count of conspiracy to commit health care fraud, six counts of health care fraud, two counts of conspiracy to defraud the United States and pay and receive health care kickbacks, and one count of soliciting health care kickbacks. If convicted, the physician faces a maximum penalty of ten years in prison for each count of conspiracy to commit health care fraud, health care fraud, and soliciting health care kickbacks, and a maximum penalty of five years in prison on each count of conspiracy to defraud the United States and pay and receive health care kickbacks.

***For more information, contact:***

**Riza I. Dagli** | 973.403.3103 | rdagli@bracheichler.com
**Keith J. Roberts** | 973.364.5201 | kroberts@bracheichler.com

## Federal Government Probing Effects of Private Equity Acquisitions in the U.S. Health Care Industry

On March 5, 2024, the Federal Trade Commission (FTC), Justice Department, and Department of Health and Human Services (the Agencies) jointly initiated a call for public comments regarding small acquisitions by private equity companies in the U.S. health-care industry. While the parties of mergers valued at more than $119.5 million must notify federal antitrust authorities and adhere to a minimum 30-day waiting period before closing, transactions below this threshold do not require reporting. This exemption has raised concerns about potential adverse effects on workers and patients alike, prompting regulatory scrutiny.

The heightened interest in private equity transactions, particularly "roll-ups" where firms make initial acquisitions and proceed to acquire multiple businesses in the same sector, is drawing attention at multiple levels. Regulatory bodies are also investigating the influence private equity firms wield over corporate boards across various industries. Of particular concern are instances where board directors, often associated with private equity firms, hold seats on rival firms within the same sector. The fear is that such cross-pollination of board memberships could diminish competitive dynamics in the marketplace.

The FTC's focus on private equity in health-care markets is evidenced by its recent legal action against U.S. Anesthesia Partners Inc. and its private equity partner, Welsh Carson Anderson & Stowe LP. The lawsuit filed on September 21, 2023 alleges monopolistic practices aimed at dominating the anesthesiology market in Texas using the "roll-up" strategy.

The public may submit comments to the Agencies until May 6, 2024.

***For more information, contact:***

**John D. Fanburg, Chair** | 973.403.3107 | jfanburg@bracheichler.com
**Edward Hilzenrath** | 973.403.3114 | ehilzenrath@bracheichler.com

## Implementation of the No Surprises Act Spurs Surge in In-Network Claims

On February 20, 2024, FAIR Health released a white paper on the implementation of the No Surprises Act (NSA). The White Paper focused on professional services in facility settings, particularly in specialties prone to surprise billing such as anesthesia, emergency medicine, pathology, and radiology.

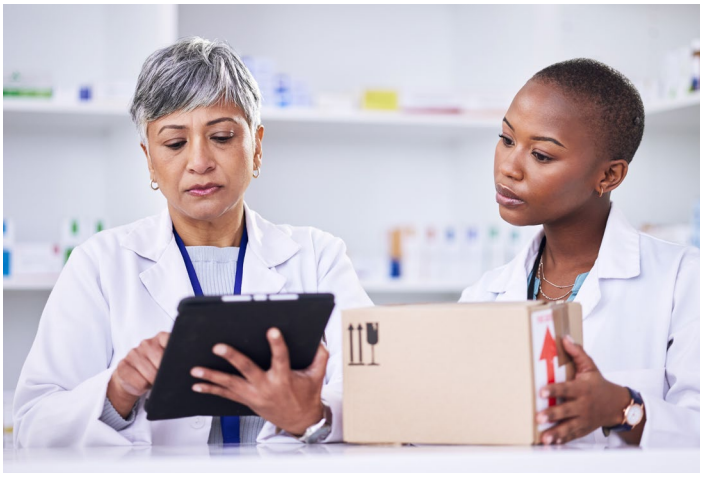
Key findings indicate a predominant trend of in-network care, albeit with varying growth rates among specialties, with radiology maintaining the highest in-network percentage and emergency medicine experiencing the largest increase. Moreover, the study reveals a decline in allowed amounts as a percentage of billed amounts for both in-network and out-of-network services over the study period. Additionally, a convergence trend between average in-network and out-of-network allowed amounts was observed.

Across all professional specialties in facility settings, the proportion of in-network care experienced a notable increase from the first quarter of 2019 to the third quarter of 2023, both nationally and in all regions. Over this period, the percentage of in-network care among all

claim lines rose by 7.0% nationally and increased 4.8% in the Northeast.

***For more information, contact:***

**Isabelle Bibet-Kalinyak, Vice Chair** | 973.403.3131 | ibibetkalinyak@bracheichler.com
**Joseph M. Gorrell** | 973.403.3112 | jgorrell@bracheichler.com



## CMS Issues Notice of Proposed Rulemaking Regarding Accrediting Organizations

On February 15, 2024, the Centers for Medicare & Medicaid Services issued a notice of proposed rule making to increase oversight of accrediting organizations ("AOs"). AOs survey over 9,000 accredited health care providers and suppliers in the Medicare/Medicaid program for compliance with health and safety requirements. CMS has identified concerns related to AO performance such as inconsistent survey results due to differing AO standards or practices, possible conflicts of interest resulting from AOs providing fee-based consulting services to providers and suppliers they accredit, and providers and suppliers that have been terminated from Medicare/Medicaid but retaining accreditation.

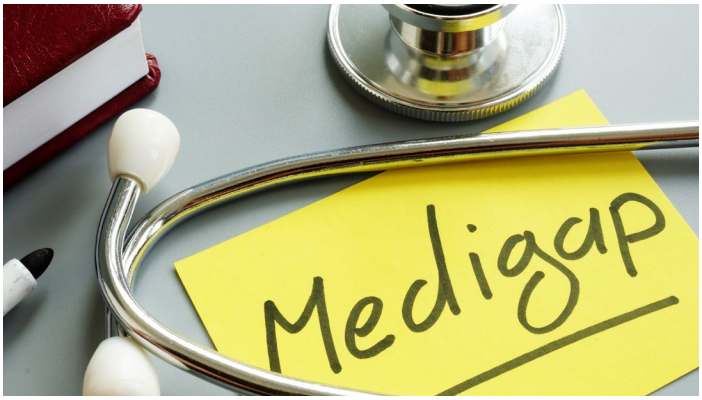
Proposed changes include holding AOs accountable to the same standards as state survey agencies, limiting fee-based consulting services AOs provide to health care facilities they accredit, and requiring AOs with poor performance to submit a publicly reported correction plan to CMS. The changes outlined in the proposed rule affects all AOs except those that accredit clinical laboratories under CLIA and non-certified suppliers. Comments to the proposed rule must be received by CMS no later than 5:00 p.m. on April 15, 2024.

***For more information, contact:***

**Keith J. Roberts** | 973.364.5201 | kroberts@bracheichler.com
**Lani M. Dornfeld, CHPC** | 973.403.3136 | ldornfeld@bracheichler.com

## OIG Issues Favorable Advisory Opinion Regarding Discounts between Medigap and PHO's

On February 26, 2024, the Office of Inspector General (OIG) issued Advisory Opinion 24-01, approving the use of a discount as part of an arrangement between a Medicare Supplement (Medigap) plan offered by a private insurance company and a preferred hospital organization (PHO) as part of a "preferred network" of hospitals. Under the proposed arrangement, the PHO would provide discounts on the otherwise-applicable Medicare Part A inpatient deductibles for the Medigap plan's policyholders and, in turn, the Medigap insurer would provide a premium credit of $100 off the next renewal premium to those policyholders who use a network hospital within the PHO's network for an inpatient stay The discount offered by the PHO would be established in advance pursuant to a written agreement, and the premium credit offered by the Medigap insurer would not be in the form of a check, deposit, or other affirmative payment to the policyholder. Additionally the Medigap plan would pay the PHO a percentage based administrative fee, based off the aggregate savings of the policyholders and consistent with fair market value, for PHO's efforts in maintaining the network of hospitals.




The OIG concluded that while the proposed arrangement could generate prohibited remuneration under the federal Anti-Kickback Statute, the OIG would not impose administrative sanctions in this case because the arrangement would be unlikely to increase costs for federal healthcare programs, is unlikely to lead to inappropriate utilization of healthcare services, and would be unlikely to impact competition or patient choice. This marks the fifth time since December 18, 2023, that the OIG has issued a nearly identical opinion on the issue of PHO discounts for Medigap policyholders. Specifically, all 5 OIG opinions allowed a Medigap

insurance company contracting with the PHO to provide discounts on the otherwise-applicable Medicare Part A inpatient deductibles for policyholders and, in turn, allowed the Medigap insurer to provide a premium credit of $100 off the next renewal premium to those policyholders who used a network hospital within the PHO's network for an inpatient stay. According to the OIG, five separate Advisory Opinions were issued because there were multiple parties to the fact pattern and each requested an Advisory Opinion specific to that party.

***For more information, contact:***

**Carol Grelecki** | 973.403.3140 | cgrelecki@bracheichler.com
**Michael C. Foster** | 973.403.3102 | mfoster@bracheichler.com


## Walgreens Owned VillageMD Rethinks its Strategy

VillageMD recently announced plans to exit the Illinois market in April 2024, only one week after VillageMD announced that it is closing all its clinics in Florida, and after already pulling out of New Hampshire and Indiana in January and Massachusetts in February. Walgreens acquired a majority stake in VillageMD in 2021, promising to open hundreds of clinics attached to Walgreens stores over the following several years, a model that Walgreens had touted as a way to encourage better collaboration between physicians and pharmacists and a way to offer convenience for patients. However, analysts have observed that Walgreens has begun to move away from this model, with more than 80 clinics that are attached to Walgreens stores either closing or set to close this spring.

Walgreens' investment in VillageMD is consistent with several other large retailers looking to take market share in healthcare services from traditional providers, including CVS, Walmart, Kroger and Amazon, who have attempted to leverage brand recognition and convenience to attract patents, each with mixed results. Clinics attached to retail stores face certain challenges, especially in highly competitive markets like Florida, including size limitation in existing stores that make it difficult to provide a wide array of medical services and the stigma felt by clinicians about working in retail store locations. As a result, Walgreens, along with Amazon, CVS and Kroger, have all begun to reassess how they operate their healthcare provider businesses and have begun to move away from the colocation model.

***For more information, contact:***

**Isabelle Bibet-Kalinyak, Vice Chair** | 973.403.3131 | ibibetkalinyak@bracheichler.com
**Jonathan J. Walzman** | 973.403.3120 | jwalzman@bracheichler.com

# HIPAA CORNER

### Change Healthcare Data Breach

Last month, healthcare technology company Change Healthcare, owned by UnitedHealth through its Optum unit, suffered a cyber-attack which is causing far-reaching consequences. Initially identified by Optum on February 21, 2024 as the unavailability of certain applications and "enterprise-wide connectivity issues," Optum later identified the issue as a "cyber security issue." On February 26, 2024, the American Hospital Association published an "AHA Cybersecurity Advisory," in order to help members "navigate this evolving incident." A number of news outlets have been monitoring the evolving information, which has now caught world-wide attention. UnitedHealth offers information on its cyber response website, which is periodically updated, including Q&A about the incident and incident response and information about UnitedHealth's advancement of temporary financial assistance through its Temporary Funding Assistance Program. Reuters has reported that UnitedHealth Group "has already been hit with at least six class action lawsuits accusing it of failing to protect millions of people's personal data from last month's hack of Change Healthcare, its payment processing unit, with more lawsuits likely to come." In a motion in Washington, D.C., the plaintiffs have requested consolidation of the cases to the Middle District of Tennessee, where Change Healthcare is headquartered. On March 22, 2024, U.S. Sen. Mark R. Warner (D-VA), a member of the Senate Finance Committee and co-chair of the Senate Cybersecurity Caucus, introduced legislation that would

provide for advanced and accelerated payments to health care providers in the event of a cyber incident, so long as the provider meets minimum cybersecurity standards. If the provider's intermediary (such as a business associate vendor) was the target of the incident, the intermediary also must meet minimum cybersecurity standards in order for the provider to receive the payments. Actions and reactions to the incident continue to evolve.

**Malicious Insider Breach Costs $4.75M**

The U.S. Department of Health & Human Services, Office for Civil Rights ("OCR") recently announced a $4.75 million settlement with a New York City hospital relating to alleged employee theft of patient information over a six-month period. By way of background, in May 2015, the New York Police Department informed the hospital that there was evidence of theft of a specific patient's medical information. The hospital thereafter conducted an investigation and discovered that, two years prior, one of its employees stole the electronic health information of over 12,517 patients and sold the information to an identity theft ring. The OCR found multiple potential violations of HIPAA by the hospital, including failures by the hospital to analyze and identify potential risks and vulnerabilities to protected health information, to monitor and safeguard its health information systems' activity, and to implement policies and procedures that records and examine system activity in information systems containing or using protected health information. In addition to the monetary settlement, the hospital is required to implement a corrective action plan and undergo two years of OCR monitoring.

In its announcement, the OCR noted: "In OCR's breach reports, over 134 million individuals have been affected by large breaches in 2023, whereas 55 million were affected in 2022. OCR recommends that health care providers, health plans, clearinghouses, and business associates that are covered by HIPAA must implement safeguards to mitigate or prevent cyber threats."

**Second Ever Ransomware Cyber-Attack Settlement**

On February 21, 2024, the OCR announced its second-ever ransomware cyber-attack settlement. The settlement resolved an OCR investigation of a Maryland-based behavioral health provider following a ransomware attack that affected the protected health information of more than 14,000 individuals. Cyber attackers infected the provider's network server and encrypted company files and patient records. The OCR found multiple violations of HIPAA, including the failure to (i) have in place an accurate and thorough analysis to determine the potential risks and vulnerabilities to electronic protected health information; (ii) implement security measures to reduce risks and vulnerabilities to a reasonable and appropriate level; and (iii) have sufficient monitoring of its health information systems' activity to protect against a cyber-attack. Under the terms of the settlement, the provider agreed to a $40,000 monetary settlement, implementation of a corrective action plan, and OCR monitoring for three years.

**HHS OCR Annual Report to Congress on HIPAA Compliance and Breaches of Patient Information**

On February 14, 2024, the OCR issued two reports to Congress for calendar year 2022, Annual Report to Congress on HIPAA Privacy, Security and Breach Notification Rule Compliance and Annual Report to Congress on Breaches of Unsecured Protected Health Information.

Highlights of the first report include:

- OCR received 30,435 new complaints alleging violations of the HIPAA Rules
- OCR resolved 32,250 complaints alleging violations of the HIPAA Rules
- OCR resolved 17 complaint investigations with Resolution Agreements and Corrective Action Plans (RA/CAPs) and monetary settlements totaling $802,500, and one complaint investigation with a civil money penalty in the amount of $100,000
- OCR completed 846 compliance reviews and required subject entities to take corrective action or pay a civil money penalty in 80% (674) of these investigations. Three compliance reviews were resolved with RA/CAPs and monetary payments totaling $2,425,640.

The second report highlights the fact that, with respect to breach events affecting more than 500 individuals that were reported to OCR in 2022, a total of approximately 41,747,613 individuals were affected. The most commonly reported category of breaches was hacking/IT incidents, with the largest of this type of breach affecting 3,300,638 individuals. The largest category by location for breaches involving 500 or more individuals was network servers.

Common deficiencies and vulnerabilities in protections noted by the OCR as areas needing improvement include:

- Conducting security risk analyses and using the results to develop and implement risk management plans
- Regularly conducting information system activity reviews
- Implementing audit controls—hardware, software and/or procedural mechanisms that record and examine system activity in information systems that contain protected health information
- Identifying and responding to suspected or known security incidents and mitigating, to the extent practicable, harmful effects of security incidents
- Implementing person or entity authentication—procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

**Cybersecurity Resource Guide Published**

Last month, the OCR and the National Institute of Standards and Technology (NIST) jointly published Special Publication (SP) 800-66 Revision 2, *Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide*.

The publication provides an overview of the HIPAA Security Rule, strategies for assessing and managing risks to electronic protected health information, suggestions for cybersecurity measures and solutions that HIPAA covered entities and business associates might consider as part of an information security program, and resources for implementing the Security Rule. Specific topic areas include:

- Explanations of the HIPAA Security Rule's Risk Analysis and Risk Management requirements
- Key Activities to consider when implementing Security Rule requirements
- Actionable steps for implementing security measures
- Sample questions to determine adequacy of cybersecurity measures to protect ePHI.

Additional resources are available on the NIST website.

***If you need assistance with your HIPAA compliance program, an OCR investigation, or a data breach incident, please contact:***

**Isabelle Bibet-Kalinyak, Vice Chair** | 973.403.3131 | ibibetkalinyak@bracheichler.com
**Lani M. Dornfeld, CHPC** | 973.403.3136 | ldornfeld@bracheichler.com

## BRACH EICHLER IN THE NEWS

Effective April 1st, the following Healthcare Law attorneys were promoted to Counsel. Congratulations **Paul J. Demartino, Jr.**, **Cynthia J. Liba**, and **Erika R. Marshall**.

On March 22, Healthcare Law Member **Keith J. Roberts, Esq.** was included in NJBIZ's 2024 "Leaders in Law" list. The Leaders in Law awards program honors legal professionals whose dedication to their occupation and to their communities is outstanding. Congratulations!

On March 8, Brach Eichler celebrated International Women's Day. We honored the incredible achievements of women around the globe and reaffirmed our dedication to gender equality. It's about uplifting and empowering each other, not just on one day, but every day.

On February 6, Healthcare Law Member **Isabelle Bibet-Kalinyak, Esq.**, issued an alert entitled, "A New Year, A New Deadline: Are You Ready to File Your Beneficial Ownership Reports Under the Federal Corporate Transparency Act?"

# ATTORNEY **SPOTLIGHT**

**Get to know the faces and stories of the people behind the articles in each issue. This month, we invite you to meet Members Carol Grelecki and Joe Gorrell.**

## CAROL GRELECKI

**What advice can you share with a client who might need your services?**

First, be open and honest about your goals and objectives. There is almost never just one way to handle a legal matter. If your attorney has a clear understanding of your goals and objectives, together you will be in the better position to choose the course that is right for you. Second, for major projects consider bringing your attorney into the planning early on in the process. An attorney may identify issues at the planning stage, which the business team may not. This will allow you to address legal issues at the outset and avoid costly delays at a later date.

**What are some best practices for healthcare clients?**

The healthcare industry is heavily regulated and the rules that apply to healthcare providers are constantly changing. To avoid legal issues, it is essential to be proactive, to have a robust and ongoing compliance program, and to invest in experts when necessary to ensure that you are keeping abreast of all regulatory requirements applicable to you.

## JOE GORRELL

**What advice can you share with a client who might need your services?**

Once you make the choice of counsel, trust that she or he has your best interests in mind and be transparent. Make sure that you provide all information that might be relevant to the representation and err on the side of disclosure, as you may not recognize what information may be helpful.

**What are some best practices for healthcare clients?**

For those providing clinical care, it is essential that you are careful to document the care that you provide, including very importantly the reasoning behind your decision making.

BRACH | EICHLER LLC
Counsellors at Law



## HEALTHCARE LAW PRACTICE | 101 EISENHOWER PARKWAY, ROSELAND, NJ 07068

### MEMBERS

**Isabelle Bibet-Kalinyak, Vice Chair** | 973.403.3131 | ibibetkalinyak@bracheichler.com
**Shannon Carroll** | 973.403.3126 | scarroll@bracheichler.com
**Riza I. Dagli** | 973.403.3103 | rdagli@bracheichler.com
**Lani M. Dornfeld** | 973.403.3136 | ldornfeld@bracheichler.com
**John D. Fanburg, Chair** | 973.403.3107 | jfanburg@bracheichler.com
**Joseph A. Ferino** | 973.364.8351 | jferino@bracheichler.com
**Joseph M. Gorrell** | 973.403.3112 | jgorrell@bracheichler.com
**Carol Grelecki** | 973.403.3140 | cgrelecki@bracheichler.com
**Edward Hilzenrath, HLU Editor** | 973.403.3114 | ehilzenrath@bracheichler.com
**Keith J. Roberts** | 973.364.5201 | kroberts@bracheichler.com
**Richard Robins** | 973.447.9663 | robins@bracheichler.com
**Jonathan J. Walzman** | 973.403.3120 | jwalzman@bracheichler.com
**Edward J. Yun** | 973.364.5229 | eyun@bracheichler.com

### COUNSEL

**Colleen Buontempo, CPC** | 973.364.5210 | cbuontempo@bracheichler.com
**Paul J. DeMartino, Jr.** | 973.364.5228 | pdemartino@bracheichler.com
**Michael C. Foster, Federal HLU Editor** | 973.403.3102 | mfoster@bracheichler.com
**Cynthia J. Liba** | 973.403.3106 | cliba@bracheichler.com
**Debra W. Levine** | 973.403.3142 | dlevine@bracheichler.com
**Erika R. Marshall** | 973.364.5236 | emarshall@bracheichler.com

### ASSOCIATES

**Vanessa Coleman** | 973.364.5208 | vcoleman@bracheichler.com

Roseland, NJ | New York, NY | West Palm Beach, FL | www.bracheichler.com | 973.228.5700

**STAY CONNECTED!** FOLLOW US