2025 | VOL. 30 | NO. 1

NYSBA

Health Law Journal

A Peer Reviewed Law Journal

A publication of the Health Law Section of the New York State Bar Association

Special Issue on Digital Health

Federal Interoperability Initiatives and Opportunities for New York State Participation

The State of Play for the Use of Online Tracking Technology in Health Care

NYS Insurers' Considerations in Using Artificial Intelligence in Underwriting or Pricing

Contents

Regular Features

Featured Articles

NYSBA

Health Law Journal

2025 | Vol. 30 | No. 1

In Each Issue

Publication and Editorial Policy

Persons interested in writing for this *Journal* are welcomed and encouraged to submit their articles for consideration. Your ideas and comments about the *Journal* are appreciated as are letters to the editor.

Publication Policy
All articles should be submitted to:

Cassandra DiNova
Email: cassandra.dinova@cdphp.com

Submitted articles must include a cover letter giving permission for publication in this *Journal.* We will assume your submission is for the exclusive use of this *Journal* unless you advise to the contrary in your letter. Authors will be notified only if articles are rejected. Authors are encouraged to include a brief biography with their submissions. Authors will be asked to sign a copyright agreement that can be found here:
NYSBA.ORG/SECTION-PUB-AUTHOR/

Editorial Policy: The articles in this *Journal* represent the authors' viewpoints and research and not that of the *Journal* Editorial Staff or Section Officers. The accuracy of the sources used and the cases cited in submissions is the responsibility of the author.

Subscriptions

This *Journal* is a benefit of membership in the Health Law Section of the New York State Bar Association.

The *Journal* is available by subscription to non-attorneys, libraries and organizations. The subscription rate is $160.00. Send your request and check to Member Resource Center, New York State Bar Association, One Elk Street, Albany, NY 12207.

Accommodations for Persons with Disabilities
NYSBA welcomes participation by individuals with disabilities. NYSBA is committed to complying with all applicable laws that prohibit discrimination against individuals on the basis of disability in the full and equal enjoyment of its goods, services, programs, activities, facilities, privileges, advantages, or accommodations. To request auxiliary aids or services or if you have any questions regarding accessibility, please contact the Bar Center at 518-463-3200.

Publication Date: January 2025

ISSN 1530-3926 ISSN 1933-8406 (online)

Message From the Chair

On October 21, the Health Law Section was pleased to welcome members to this year's Fall Meeting program, chaired by Anoush Koroghlian-Scott of Lippes Mathias LLP, and Heather Butts of Columbia University Mailman School of Public Health, and held at the Gideon Putnam in Saratoga Springs. Attendees were very positive about the setting and fall environs that added to the pleasant and convivial experience. The fall program kicked off with meetings of section committees, including the Legislative Committee chaired by Mark R. Ustin of Farrell Fritz, and the Public Health Committee chaired by Heather Butts. As described in brief below, all five panel programs presented by section members and invited guest speakers were very well received based upon both oral feedback and written evaluations.

The morning program opened with a panel addressing the New York Health Equity Reform 1115 Waiver Amendment approved by CMS that includes nearly $6 billion of federal funding for social care networks. Chaired by Heather Butts, panel members hailing from both government and other sectors engaged in spirited discussion with those in attendance on how the waiver would be implemented, including meeting the challenge of outreach to providers.

An interdisciplinary panel on medical aid in dying in the morning session featured several members of the New York State Bar Association 2023-2024 Medical Aid in Dying Task Force established by Immediate Past NYSBA President Richard Lewis, including Task Force Chair Mary Beth Morrissey of Yeshiva University, Mark R. Ustin, John Dow of Trinity Health, Edward McArdle of SUNY Upstate and Cornell Law School, and Heather Butts. Panelists discussed current legal and ethical issues concerning MAID that will continue to draw attention. They were joined by Paul Heasley, MD, Chief Medical Officer, Community Hospice, Albany, N.Y. Panelists called attention to current inequities in access to palliative and end-of-life care, and cited research suggesting that enactment of a Medical Aid in Dying Law in New York would not necessarily ensure equitable access to care without adequate planning for expected challenges in implementation. Mary Beth Morrissey, John Dow, and Ed McArdle have been invited to present at the Elder Law Section Annual Meeting program in January on the subject of medical aid in dying.

The afternoon session featured an interdisciplinary panel on maternal health, chaired by Mary Beth Morrissey, building on the recent special issue of this *Health Law Journal* on the same topic. Immediate Past President Lisa Hayes and fellow presenters Dorothy Shuldman of Phillips Lytle LLP, Mary Breda Morrissey, MD, of the Yale New Haven Health System, and Cornell Law Student (3L) Cauolyn Baptiste, called attention to evidence of structural racism contributing to inequities in access to care for Black women. Discussion was also had on the impact of private equity on maternal health outcomes in the United States.

In the second afternoon panel, William P. Keefer of Phillips Lytle LLP, Colleen R. Pierson of Garfunkel Wild, P.C., and Chaya Rosenbaum of Weiss Zarett Brofman Sonnenklar & Levy, P.C., provided an analysis of the *Loper-Bright* decision, the seminal case overturning *Chevron*. The discussion included an overview of the case law that led up to *Loper-Bright,* key provisions of the decision, as well as the possible impacts of the decision on the health care industry. The panel discussed the implications of *Loper-Bright* on long-term care, specifically the nursing home industry, the FTC rule decisions, and possible areas of future administrative law litigation in health care.

The fall program closed with a presentation by Linda J. Clark of Barclay Damon LLP on the Office of the Medicaid Inspector General (OMIG). The Health Law Section OMIG Working Group is preparing a formal report for submission to the NYSBA House of Delegates this January, and will also present at the Annual Meeting of the Health Law Section.

Finally, several members of the Health Law Section are serving on President Domenick Napoletano's opioid Task Force, including Mary Beth Morrissey, who is chairing the Task Force, Margaret Davino, and Lisa Smith. The Task Force will deliver an informational report to the House of Delegates by January 2025, and a panel presentation is also planned for the Annual Meeting.

In closing, we encourage all our Health Law Section members and colleagues to join us at the Annual Meeting to continue the important work of building collegiality and solidarity among our section members, as well as reaching across the aisle to our NYSBA colleagues in other sections and committees!

Mary Beth Quaranta Morrissey

In the Legislature

By Michael A. Paulsen

As of this writing, the 2024 presidential election and state general election are well underway for all 26 seats in the U.S. House of Representatives, all 63 seats in the New York State Senate and all 150 seats in the New York State Assembly. In New York, the outcome of the general election is unlikely to significantly alter the balance of power in Albany. The Assembly is expected to remain overwhelmingly under Democratic control and the Senate is also expected to remain under Democratic control.

From a fiscal perspective, New York passed a $239 billion budget in April, increasing spending by 7.8%, without imposing new taxes or other significant revenue raising actions. The state currently has a projected budget deficit of $4 billion for Fiscal Year (FY) 2026, which is projected to grow increase to $16 billion by FY 2028.

Looking forward, we expect the following health care issues to be under consideration during the upcoming New York State legislative session.

Managed Care Organization Tax

The FY 2025 Enacted Budget authorized the commissioner of health to pursue federal approval for a managed care organization (MCO) tax. Funds generated from the MCO tax will be held in a new "Healthcare Stability Fund" to be available to fund the non-federal share of increased payments to managed care providers, reimbursing the general fund for expenditures incurred in the Medicaid program, and supporting capital projects funds.

It is widely understood that the MCO tax was modeled on a similar tax implemented in California, which applies the tax to managed care organizations and commercial insurers but imposes different rates between Medicaid plans and non-Medicaid plans to minimize the impact on the commercial insurance market. If approved by Centers for Medicare and Medicaid Services (CMS), the MCO tax is expected to generate $4 billion in federal funding annually for the next three years. While the Department of Health submitted a waiver application to CMS to implement the tax, no details on how the tax would be structured or how the increased revenue would be spent have been released.

If approved, the MCO tax will take a significant amount of pressure off the impact of the state's Medicaid spending on the overall budget, allowing for Medicaid provider rate increases and increased spending within the program, while minimizing the need to implement policies that generate savings. However, a more immediate concern is whether the MCO tax will even be approved by CMS, as CMS questioned whether the California model meet the spirit of the federal regulations in the approval letter to California. If the MCO tax is not approved, the state will face another year of seeking to identify savings in the Medicaid program. Another significant concern is if the MCO tax is approved, it would need to be reauthorized by CMS every three years, meaning that any MCO tax revenue used for reoccurring spending, such as provider rate increases, could put significant strain on the state's finances in the future if the tax is modified or not reauthorized.

Commission on Future of Health Care

First announced in the governor's 2023 State of the State address, the Commission on the Future of Health Care was tasked with developing strategic recommendations to transform the health care system in New York State. The commission is expected to release its first recommendations before the end of 2024. It is widely understood that the commission recommendations regarding policy, regulatory and reimbursement reforms would be made to the governor to inform the development of the Sate Fiscal Year (SFY) 26 Executive Budget.

As the commission has started meeting and public summaries of the meetings have been released, our understanding is that the focus of the commission has on taking a longer-term view of how to align financial and policy incentives to improve patient outcomes and experience in the New York health care delivery system across the continuum of services, how to strengthen the health care workforce, and address health equity. It is also taking a broader look at health care costs and spending beyond Medicaid. While the actual recommendations of the commission are unknown at this time, it is possible that the recommendations could significantly alter New York's health care delivery system.

Artificial Intelligence

As the capabilities of artificial intelligence (AI) continue to expand, there is a general recognition that there are risks associated with the increased use and application of AI, particularly in health care. New York has started to take steps to

regulate the use of AI technology, most recently enacting the SAFE for Kids Act, which regulates social media platforms' ability to present addictive algorithmic feeds to children.[1]

In the 2023-24 legislative session, legislative members introduced over 50 bills that regulate the use of AI, many of which are not specific to health care but would be applicable to health care providers using AI. We expect that AI regulation specific to the use in health care will be introduced in the upcoming session, following trends in other states. Based on a review of introduced and passed legislation related to AI and health, potential themes include:

- Requiring patient notification of the use of AI and allowing for patients to opt out of its use.
- Requiring providers to monitor AI tools that are being used, including decision validation and/or possess the power to override AI when deemed appropriate.
- Requiring all health insurers to disclose the use of AI in their utilization review process and any associated algorithms/training sets to their department of transparency.[2]
- Requiring AI-generated patient communication to include a disclaimer and instructions about how to contact a human health care provider.

Michael A. Paulsen is of counsel in the Albany office of Manat, Phelps, & Phillips, LLP, where he focuses on legal, regulatory and legislative issues for health care providers.

Endnotes

1. New York General Business Law § 1500 *et seq*.
2. *See* A.B. 9149 (2024).

In the New York State Agencies

Compiled by Nicola Coleman and Binny Seth

6/18/24

Minimum Standards for Form, Content and Sale of Health Insurance, Including Standards of Full and Fair Disclosure

Notice of Adoption. The Department of Financial Services amended Part 52 (Regulation 62) of Title 11 N.Y.C.R.R. to comport with changes made to Insurance Law § 1117 by Chapter 655 of the Laws of 2023. Filing Date: May 29, 2024. Effective Date: June 18, 2024. *See* N.Y. Register June 18, 2024.

Enterprise Risk Management, Own Risk and Solvency Assessment; Group-Wide Supervision

Notice of Adoption. The Department of Financial Services amended Part 82 (Regulation 203) of Title 11 N.Y.C.R.R. to implement Chapter 344 of the laws of 2023, which imposed an annual GCC filing requirement. Filing Date: June 4, 2024. Effective Date: June 18, 2024. *See* N.Y. Register June 18, 2024.

Notice of Expiration

The following notice has expired and cannot be reconsidered unless the Department of Health publishes a new notice of proposed rulemaking:

The Department of Health, *Perinatal Services, Perinatal Regionalization, Birthing Centers and Maternity Birthing Centers*, I.D. No. HLT-22-23-00011-P. Proposed on May 31, 2023. Expired on May 30, 2024. *See* N.Y. Register June 18, 2024.

6/26/24

Provider Enrollment and Collection of Patient Consent to Access Medicaid Confidential Data in the Statewide Health Information Network for New York (SHIN-NY)

Notice of Proposed Rule Making. The Department of Health proposed to amend § 504.9 of Title 18 N.Y.C.R.R. to clarify that providers of medical goods and services, rather than the Qualified Entities, are required to enroll in the Medicaid program. *See* N.Y. Register June 26, 2024.

7/3/24

Contingent Reserve Requirements for Managed Care Organizations (MCOs)

Notice of Proposed Rule Making. The Department of Health proposed to amend § 98-1.11(e) of Title 10 N.Y.C.R.R. to maintain the contingent reserve requirement at 7.25% through 2025 applied to the Medicaid Managed Care, HIV SNP and HARP programs. *See* N.Y. Register July 3, 2024.

Relating to Residential Treatment Facilities (RTF)

Notice of Adoption. The Office of Mental Health repealed Part 583, added a new Part 583 and amended Part 584 of Title 14 N.Y.C.R.R. to provide clarity and uniformity relating to RTFs and to implement Chapter 58 of the laws of 2020. Filing Date: June 12, 2024. Effective Date: July 3, 2024. *See* N.Y. Register July 3, 2024.

7/10/24

Statewide Health Information Network for New York (SHIN-NY)

Notice of Adoption. The Department of Health amended Part 300 of Title 10 N.Y.C.R.R. to establish the State Designated Entity and Enhancing SHIN-NY Efficiency and Flexibility. Filing Date: June 25, 2024. Effective Date: July 10, 2024. *See* N.Y. Register July 10, 2024.

Notice of Expiration

The following notice has expired and cannot be reconsidered unless the Department of Health publishes a new notice of proposed rulemaking:

The Department of Health, *Humane Euthanasia of Animals*, I.D. No. HLT-25-23-00002-P. Proposed on June 21, 2023. Expired on June 20, 2024. *See* N.Y. Register July 10, 2024.

Emergency Medical Services Equipment Requirements for Certified Ambulance and Emergency Ambulance Service Vehicles

Notice of Proposed Rule Making. The Department of Health proposed to repeal § § 800.24, 800.25 and 800.26 and add new § § 800.24, 800.25 and 800.26 to Title 10 N.Y.C.R.R. to update requirements to meet current industry standards

that address patient and provider safety and manufacturing guidelines. *See* N.Y. Register July 10, 2024.

7/17/24

Credit for Reinsurance

Notice of Adoption. The Department of Financial Services amended Part 125 (Regulation 17, 20 and 20-A) of Title 11 N.Y.C.R.R. to prescribe the collateral requirements for reinsurance reserve credit. Filing Date: July 02, 2024. Effective Date: July 17, 2024. *See* N.Y. Register July 17, 2024.

7/31/24

Admission and Discharge Criteria for Psychiatric Inpatient Units of General Hospitals

Notice of Revised Rule Making. The Office of Mental Health amended Part 580 of Title 14 N.Y.C.R.R. to standardize admissions and discharges. *See* N.Y. Register July 31, 2024.

Admission and Discharge Criteria for Comprehensive Psychiatric Emergency Programs

Notice of Revised Rule Making. The Office of Mental Health amended Part 590 of Title 14 N.Y.C.R.R. to standardize admissions and discharges. *See* N.Y. Register July 31, 2024.

Admission and Discharge Criteria for Hospitals for Persons with Mental Illness

Notice of Revised Rule Making. The Office of Mental Health amended Part 582 of Title 14 N.Y.C.R.R. to standardize admissions and discharges. *See* N.Y. Register July 31, 2024.

Pathway to Employment

Notice of Proposed Rule Making. The Office for People with Developmental Disabilities amended Subpart 635-10 of Title 14 N.Y.C.R.R. to update the pathway to employment regulations as New York becomes an employment-first state. *See* N.Y. Register July 31, 2024.

Supported Decision-Making

Notice of Proposed Rule Making. The Office for People with Developmental Disabilities added Part 634, amended Parts 624, 629, 633, 635, 636, 679 and repealed § 681.13 of Title 14 N.Y.C.R.R. to effectuate the adoption of supported decision-making practices within the OPWDD service system. *See* N.Y. Register July 31, 2024.

9/4/24

Exemption of Earned Income and Public Assistance (PA) and Supplemental Nutrition Assistance Program (SNAP) Employment Program Requirements Updates

Notice of Adoption. The Office of Temporary and Disability Assistance amended § and Part 385 of Title 18 N.Y.C.R.R. to update state regulations pertaining to exemption of earned income and PA and SNAP employment program requirements consistent with updated federal and state laws. Filing Date: August 20, 2024. Effective Date: September 4, 2024. *See* N.Y. Register September 4, 2024.

9/18/24

Notice of Expiration

The following notice has expired and cannot be reconsidered unless the Office of Mental Health publishes a new notice of proposed rulemaking:

COVID-19 Vaccination Program. Proposed on August 30, 2023. Expired on August 29, 2024. *See* N.Y. Register September 18, 2024.

Technical Amendments to State Regulations Updating the Names of State Agencies and Replacing Obsolete and Stigmatizing Terms

Notice of Proposed Rule Making. The Office of Temporary and Disability Assistance proposed to update state regulations by replacing obsolete and stigmatizing terms. *See* N.Y. Register September 18, 2024.

9/25/24

Voluntary Certification of Recovery Residences in New York State

Notice of Adoption. The Office of Alcoholism and Substance Abuse Services added Part 860 to Title 14 N.Y.C.R.R. to establish the requirements for recovery residences certified by OASAS. Filing Date: September 9, 2024. Effective Date: September 25, 2024. *See* N.Y. Register September 25, 2024.

Adult Home Admission and Reporting Requirements

Notice of Adoption. The Department of Health amended § § 487.4 and 487.10 of Title 18 N.Y.C.R.R. to clarify the preadmission screening process and strengthen the reporting of residents with serious mental illness diagnoses. Filing Date: September 6, 2024. Effective Date: December 24, 2024. *See* N.Y. Register September 25, 2024.

Onsite Wastewater Treatment System Waiver Requirements

Notice of Proposed Rule Making. The Department of Health amended Part 75 of Title 10 N.Y.C.R.R. to clarify availability of waivers from statewide requirements regarding installation and operation of wastewater treatment systems. *See* N.Y. Register September 25, 2024.

Notice of Expiration

The following notice has expired and cannot be reconsidered unless the Office of Mental Health publishes a new notice of proposed rulemaking:

Use of Telehealth in Crisis Stabilization Centers. Proposed on September 6, 2023. Expired on September 5, 2024. *See* N.Y. Register September 25, 2024.

Standard Utility Allowances (SUAs) for the Supplemental Nutrition Assistance Program (SNAP)

Notice of Emergency/Proposed Rule Making. The Office of Temporary and Disability Assistance amended § 387.12(f)(3)(v)(a)-(c) of Title 18 N.Y.C.R.R. to set forth the federally-approved SUAs as of 10/1/2024. Filing Date: September 10, 2024. Effective Date: October 1, 2024. *See* N.Y. Register September 25, 2024.

10/2/24

Hospital Cybersecurity Requirements

Notice of Adoption. The Department of Health added a new § 405.46 to Title 10 N.Y.C.R.R. to create cybersecurity program requirements at all Article 28 regulated facilities. Filing Date: September 13, 2024. Effective Date: October 2, 2024. *See* N.Y. Register October 2, 2024.

Reproductive Health Care Standards

Notice of Adoption. The Department of Health amended Part 12 of Title 10 N.Y.C.R.R. and § 505.2(e) of Title 18 N.Y.C.R.R. for reconciliation with Article 25-a of the Public Health Law and alignment with evidence-based clinical guidelines. Filing Date: September 13, 2024. Effective Date: October 2, 2024. *See* N.Y. Register October 2, 2024.

Disease Outbreak Investigation and Response Clarifications

Notice of Adoption. The Department of Health amended § 2.6 of Title 10 N.Y.C.R.R. to authorize NYSDOH to provide flexibilities to local health departments to prioritize reportable diseases that need to be fully investigated. Filing Date: September 13, 2024. Effective Date: October 2, 2024. *See* N.Y. Register October 2, 2024.

Relating to the Personalized Recovery Oriented Services (PROS)

Notice of Proposed Rule Making. The Office of Mental Health proposed to repeal Part 512 and add a new Part 512 to Title 14 N.Y.C.R.R. to align the PROS program with the State Plan Amendment. *See* N.Y. Register October 2, 2024.

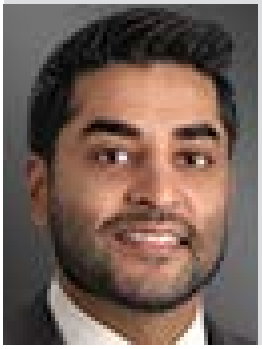
10/9/24

Principle-Based Reserving

Notice of Adoption. The Department of Financial Services amended Part 103 (Regulation 213) of Title 11 N.Y.C.R.R. to adopt the 2024 Valuation Manual. Filing Date: September 24, 2024. Effective Date: October 9, 2024. See N.Y. Register October 9, 2024.

Specialty Hospitals

Notice of Adoption. The Office for People with Developmental Disabilities amended Part 680 of Title 14 N.Y.C.R.R. to clarify requirements and better meet needs of individuals with intellectual and developmental disabilities seeking treatment at specialty hospitals. Filing Date: September 19, 2024. Effective Date: October 9, 2024. See N.Y. Register October 9, 2024.



Nicola Coleman and **Binny Seth** both participate in the Health and FDA Business Group and the Insurance Regulatory and Transaction Group at Greenberg Traurig's Albany office, where they both focus on health care issues, including regulatory, contracting, transactional and compliance matters. Prior to joining the firm, Ms. Coleman served as deputy counsel for the New York State Senate and as an associate counsel for the New York State Assembly, as well as counsel for the New York Department of Health during the creation of the Health Insurance Marketplace. Mr. Seth's past experience includes serving as in-house counsel to one of the largest Medicaid managed care organizations in New York.

New York State Fraud, Abuse, and Compliance Developments

Edited by Margaret M. Surowka

New York State Department of Health Medicaid Decisions

Compiled by Ron L. Oakes

Courtesy Transportation Services, Inc. (Decision After Hearing, June 20, 2024, Matthew C. Hall, ALJ)

Appellant is an ambulette and transportation provider operating in New York. The New York State Office of the Medicaid Inspector General (OMIG) conducted a data match desk audit of transportation services paid by the Medicaid program for the period of March 1, 2012 through December 31, 2015. In its revised final audit report, OMIG identified overpayments in the amount of $178,317.64 in four categories: (1) Transportation Billed Fee-for-Service During an Inpatient Stay; (2) Transportation Claims for Ambulette Services With Unqualified/Disqualified Driver License; (3) Transportation Claims for Ambulette Services With Incorrect/Missing Driver's License; and (4) Transportation Claims for Ambulette Services with Incorrect/Missing Vehicle License Plates.

At hearing, Administrative Law Judge (ALJ) Hall considered whether OMIG's determination to recover Medicaid program overpayments from Appellant was correct. Appellant did not present any evidence or arguments to challenge OMIG's determinations at hearing, but suggested "that the commencement of the audit, years after the events covered by the audit, is unfair . . . [because] such an audit is difficult to defend and 'sets up the OMIG for a windfall.'" *See* Decision at 12. In response to this argument, ALJ Hall noted that the audit was timely conducted and dismissed Appellant's contention.

After confirming OMIG's determinations in each of the four categories of identified overpayments, ALJ Hall concluded that Appellant failed to meet its burden to prove entitlement to payment for the disallowed claims. As such, the disallowance in the amount of $178,317.64 was affirmed.

United Hebrew Geriatric Center (Decision, June 28, 2024, Natalie J. Bordeaux, ALJ)

Appellant is a residential health care facility (RHCF) located in New Rochelle, New York. OMIG conducted an audit of the Medicaid rates paid to Appellant from January 1, 2013 through December 31, 2017. The audit consisted of a review of Appellant's records supporting the capital portion of its cost report RHCF-4 for calendar years 2011 through 2015.

On July 18, 2022, OMIG issued a final audit report that identified overpayments attributable to OMIG's audit determination to offset Appellant's interest expense reported in its 2015 cost report with the investment income it received that year from selling an investment property. Appellant purchased the property in question in 1999 and then transferred it to a related organization on January 20, 2007. The property was then sold in March 2015 for a net profit of $211,566.

As a procedural matter, after a hearing to contest the overpayment determination was scheduled and rescheduled, both parties requested a decision without a hearing. In this request, the parties only disputed OMIG's application of the applicable regulatory provision (10 N.Y.C.R.R. § 86-2.20(c)(1)) and § 202.2(C) of the Provider Reimbursement Manual (PRM-1), which formed the basis for the overpayment findings. In response to the request, ALJ Bordeaux found that there were no material facts in dispute and the request for a decision without a hearing was granted. *See* 18 N.Y.C.R.R. § 519.23(a).

In a brief to support its position, Appellant argued that the gain on the sale of the property was not realized by Appellant, but rather by the related organization, and should not be recognized as income. ALJ Bordeaux noted that the PRM-1 provides that any gain or loss realized by a related party when an asset is sold or otherwise disposed of by a related organization must be included in the provider's cost. *See* PRM-1 § 1011.3. Moreover, Appellant acquired the property with patient care funds, but never used it for patient-related services. Accordingly, the ALJ found that gains from its ultimate sale were properly classified by OMIG as investment income. *See* 10 N.Y.C.R.R. § 86-2.20(c)(1); PRM-1 § 202.2(C).

Appellants remaining arguments asserted that because the property was a depreciable asset, any income from its sale could not be recognized as it occurred after December 1, 1997. *See* PRM-1 § 130. These arguments were also rejected by the ALJ as unsupported by law. ALJ Bordeaux noted that the PRM-1 establishes that depreciation should be included in payment for services and that gains on depreciable assets from changes of ownership of a facility as an ongoing operation after December 1, 1997, should not be recognized. *See* PRM-1 § § 100, 104.14(B). However, the ALJ pointed out that the depreciable type assets to be considered in provider

payments are those used to provide services to beneficiaries and the property in question was unrelated to patient care.

Based on the information presented, the ALJ determined that Appellant failed to establish that OMIG's determination was not correct, and affirmed OMIG's determination to reduce Appellant's interest expense reported in its 2015 RHCF-4 cost report by investment income of $211,566.

In the Matter of the Appeal of Jewish Home and Infirmary of Rochester, Inc. (Decision After Hearing, July 2, 2024, Kimberly A. O'Brien, ALJ)

Appellant is a RHCF located in Rochester, New York. OMIG performed a field audit to review Appellant's cost reports as the basis of the capital portion of its Medicaid reimbursement rates for calendar years 2013 through 2016. On February 26, 2020, OMIG issued a final audit report that included findings and disallowances in four categories, but only one category was in dispute at hearing: "Gain on Extinguishment of Debt." This finding applied to the treatment of Appellant's gain on mortgage forgiveness and resulted in a disallowance of $994,285.

The main issue presented at hearing was the particular regulatory provision pertaining to the treatment of interest expense (10 N.Y.C.R.R. § 86-2.20), which applied to Appellant's mortgage at the time it was forgiven. As relevant to the issues presented at hearing, the Medical Care Facilities Finance Agency (MCFFA), succeeded by the Dormitory Authority of the State of New York (DASNY), and the Village of East Rochester Housing Authority (VERHA) were public authorities/public benefit corporations authorized to issue bonds. *See* Decision at 4-5. Appellant secured a mortgage in 1983 with bonds issued by MCFFA/DASNY and then, in 2002, refinanced the mortgage with bonds issued by VERHA. The interest costs and depreciation associated with Appellant's mortgage were included in the capital portion of Appellant's relevant Medicaid rate years. The structure of the VERHA bond agreement permitted Appellant to pay off the bonds in August 2015, nearly 10 years before the mortgage's maturity date of June 1, 2024. As a result, the mortgage's remaining principal was forgiven and Appellant realized a gain on extinguishment of its debt totaling $10,233,871. The manner in which the gain is treated is dependent on the applicable provision of 10 N.Y.C.R.R. § 86-2.20. On one hand, subsection (c) would recognize the gain in a single year, resulting in a Medicaid reimbursement reduction of $460,000, and in contrast, subsection (f), which governs mortgage interest rates to public finance authority, requires that the amount forgiven "be capitalized as a deferred asset and amortized over the remaining mortgage life, as a reduction to the facility's capital expense," and would result in a reimbursement reduction of roughly $6 million. *See* 10 N.Y.C.R.R. § 86-2.20(c), (f); Decision at 10-11.

At hearing, Appellant first argued that subsection (f) of 10 N.YC.R.R. § 86-2.20 did not apply because VERHA was not a public authority, as it is not listed as such by the Office of State Comptroller and it is not governed by the Public Authorities Law to provide nursing home financing. ALJ O'Brien noted that VERHA was in fact a public finance authority within the meaning of 10 N.Y.C.R.R. § 86-2.20(f) and quickly rejected Appellant's argument as unsupported by persuasive authority.

ALJ O'Brien considered testimony from Appellant's chief executive officer and chief financial officer, who testified that prior to undertaking an $80 million construction project, they met with the Department of Health's (DOH) Bureau of Long Term Care Reimbursement (BLTCR) regarding Appellant's Certificate of Need (CON) application. They further testified that at that meeting, BLTCR had provided verbal confirmation that subsection (c) of 10 N.Y.C.R.R. § 86-2.20 applied, Appellant later sent a letter to BLTCR to confirm its understanding that subsection (c) applied, and that Appellant submitted cost reports and obtained financing and CON approval for its project, based on the understanding that subsection (c) applied. ALJ O'Brien dismissed the relevance of Appellant's testimony, noting that the prospective rates set by BLTCR are provisional and subject to audit by OMIG.

After considering the matter, ALJ O'Brien agreed with OMIG that subsection (f) of 10 N.Y.C.R.R. § 86-2.20 applied to Appellant's mortgage forgiveness and affirmed OMIG's determination regarding the audit finding for "Gain on Extinguishment of Debt."

Bushwick Center for Rehabilitation and Health Care (Decision After Hearing, July 10, 2024, John Harris Terepka, ALJ)

Appellant is a RHCF located in Brooklyn, New York that operates three adult day health care (ADHC) programs and a nursing home. At issue in this audit was the capital portion of Appellant's RHCF cost reports (RHCF-4) submitted for the 2012 through 2016 calendar years. These cost reports were used to determine the capital portion of Appellant's Medicaid reimbursement rate for the period of January 1, 2014 through December 31, 2018.

On May 22, 2023, OMIG issued a final audit report that identified several disallowances of reported property costs and the determination to recover $1,353,722 in Medicaid overpayments. Of the findings contained in the final audit report, two were at issue at hearing: (1) real estate tax disallowance; and (2) moveable equipment rental disallowance.

Real estate tax disallowance was a property expense disallowance related to Appellant including real estate taxes for offsite parking lot leases in its reported property costs. OMIG disagreed with this cost reporting, pointing out that

real property leases entered into after March 10, 1975 were not reimbursable. See 10 N.Y.C.R.R. § § 86-2.17(a), (d), 86-2.21(f)(3). ALJ Terepka noted that real estate taxes for the parking lots were billed to and paid by the owner, not Appellant. At hearing, Appellant argued without providing supportive documentation, that a facility sale with change in its operator set forth in a CON approved by DOH, included sale of the parking lots. In addition to the lack of evidence, ALJ Terepka dismissed the argument finding Appellant failed to establish any approval for costs associated with offsite parking leases as capital reimbursement. ALJ Terepka also dismissed Appellant's assertion that a City of New York parking space mandate for nursing homes also legally required it to pay real estate taxes, as it is the owner, not Appellant, that must pay the taxes. As such, OMIG's determination to disallow the real estate taxes as a property cost was affirmed.

The movable equipment rental disallowance was another property expense disallowance which stemmed from Appellant reporting rental expenses for laundry equipment it leased as part of a service agreement for "all necessary [l]aundry [s]ervices, supplies and equipment." *See* Decision at 8. OMIG disallowed the reported costs on the grounds that equipment rentals that are part of a service agreement with an unrelated company are operating costs and not includable in the property component of the rate as they represent a capital cost to the vendor and not the Appellant. *See* PRM-1 § § 2806.1(C), 2806.3(B). Even though the washers and dryers were leased under a separate agreement, OMIG determined the lease was part of Appellant's service agreement because Appellant did not have the required "possession, use and enjoyment," of the equipment as it was installed at Appellant's facility specifically for the vendor to provide "all necessary [l]aundry [s]ervices, supplies and equipment." *See* PRM-1 § 2806.1(C).

At hearing, Appellant asserted that it met the requirements for laundry equipment costs in PRM-1 because: (1) the equipment was leased; (2) it was installed at its facility; and (3) a separate charge was specified for the lease in its vendor agreement. *See* PRM-1 § 2806.3(B). ALJ Terepka rejected this argument and noted that Appellant failed to mention an example set forth in the same PRM-1 provision that specifically established that "[a] cleaning service's charges for both housekeeping service and for the rental of equipment kept at the hospital for the use of the cleaning service staff is not [a capital-related cost], because the hospital does not have "possession, use and enjoyment" of the equipment." *See* Decision at 10. Appellant argued that provisions in the agreement requiring Appellant to provide electric, gas, and water hookups, and permitting Appellant's use of the machines "in a careful manner and only in connection with the normal operation of its usual activities" demonstrate that the vendor had given over possession of the laundry equipment. *See* Decision at 11. ALJ Terepka rejected these arguments, noting that the agreement also leaves all maintenance and repairs, including responsibility for, and control of, the laundry equipment to the vendor. The ALJ further noted that Appellant failed to provide an explanation of what normal operation of its usual activities – beyond the "all necessary laundry services" provided for in the agreement – that required Appellant's possession, use, and enjoyment of the equipment. *See* Decision at 11.

Appellant next argued that OMIG ignored the fact that the list of factors evidencing a lease agreement in PRM-1 § 2806.1(C) represent guidelines and not an absolute checklist. Appellant asserted that OMIG relied on the factor regarding multiple agreements, to the exclusion of all other guidance. This argument was also rejected by the ALJ, who noted that OMIG had not asserted that the existence of two agreements mandated the disallowance and "all other guidance on this issue" supports OMIG's determination in this case. *See* Decision at 12. ALJ Terepka concluded that Appellant failed to establish OMIG's application of the guidelines was inconsistent with the disallowance or an unreasonable exercise of its authority to determine allowable costs. *See* 10 N.Y.C.R.R. § 86-2.17(d).

Finally, Appellant asserted that it did not report the change when it began including the lease expense in the property component because it only began including it in 2012. ALJ Terepka pointed out that in Appellant's 2007 operating base year, it included laundry service in its operating expenses and only began reporting the laundry equipment lease as a property cost when changes to the operating rate methodology in 2012 made it favorable for subsequent rate years. The ALJ found that OMIG correctly determined that the laundry service continue to be reimbursed in the operating portion of the rate and Appellant failed to meet its burden of proving that OMIG's application of PRM-1 was incorrect. Based on these findings, including the lease expenses in the property costs resulted in duplicate reimbursement for the years under audit.

Therefore, OMIG's property expense disallowances were affirmed.

New York State Attorney General Press Releases

Compiled by Dena M. DeFazio, AbiDemi M. Donovan, Tricia C. Lu, and Amanda N. Rhodes

Attorney General James Secures $86 Million Multistate Settlement in Principle With Indivior for Its Role in the Opioid Crisis (July 26, 2024)

https://ag.ny.gov/press-release/2024/attorney-general-james-secures-86-million-multistate-settlement-principle

The Office of the Attorney General (OAG) announced an $86 million multistate settlement in principle with opioid manufacturer Indivior for its role in the opioid epidemic. The settlement in principle will provide New York and the other participating states with

funds to be used for opioid addiction treatment, recovery, and prevention programs. The indivior settlement in principle is just one among several settlements totaling more than $2.7 billion that the OAG has recovered from opioid manufacturers and other actors.

Attorney General James Urges New Yorkers To Use Free Credit Monitoring and Identity Theft Protection Services in Aftermath of Change Healthcare Cyberattack (July 9, 2024)

https://ag.ny.gov/press-release/2024/attorney-general-james-urges-new-yorkers-use-free-credit-monitoring-and-identity

In the wake of the Change Healthcare data breach that exposed millions of New Yorkers' personal information, the company is offering two years of free credit monitoring and identity protection services that will allow consumers to be on the lookout for potential warning signs that bad actors are using their medical information. A consumer alert issued by Attorney General James urges anyone who believes their information may have been compromised to use the free credit monitoring and identify theft protection services.

Attorney General James Announces Indictment of Orange County Transportation Company for Stealing Over $2.3 Million From Medicaid (July 3, 2024)

https://ag.ny.gov/press-release/2024/attorney-general-james-announces-indictment-orange-county-transportation-company

The OAG announced the arrests and indictments of three Orange County residents and their company for an alleged scheme calculated to have stolen over $2.3 million from the state's Medicaid program. The company operated as a medical transportation provider and allegedly used the business to overcharge Medicaid millions of dollars in fees by billing for fake trips and adding fake tolls to rides they did provide. The three stand accused of also having made kickback payments to Medicaid recipients in order to recruit more passengers to increase their fraudulent billing.

Attorney General James Announces Arrest of Tompkins County Transportation Company Owner for Stealing Over $1 Million from Medicaid (July 3, 2024)

https://ag.ny.gov/press-release/2024/attorney-general-james-announces-arrest-tompkins-county-transportation-company

The OAG announced the arrest of a Tompkins County resident who is alleged to have stolen over $1 million from Medicaid by using fictitious billing and an illegal kickback scheme to overcharge for transportation services offered through his medical transportation company. The defendant is alleged to have exploited the system by paying Medicaid recipients to use his service, submitting claims for fictitious trips, and significantly inflating the mileage of trips that did happen.

Attorney General James Announces Indictments of Rensselaer and Orange County Medical Transport Companies for Stealing Over $4.4 Million From Medicaid (June 27, 2024)

https://ag.ny.gov/press-release/2024/attorney-general-james-announces-indictments-rensselaer-and-orange-county

The OAG announced the indictments and arrests of five Medicaid-contracted transportation providers, and seven companies owned by them, alleged to have stolen over $4.4 million in Medicaid funds through fictitious billing and illegal kickback schemes. The indictments allege that a key component of the defendants' operations was kickback schemes wherein the defendants illegally recruited and paid kickbacks to Medicaid recipients for signing up with their companies and for requesting rides from addresses farther away from where they lived. The defendants are further alleged to have engaged in money laundering using shell companies in order to obtain the illegal proceeds of their frauds in cash and distribute the kickbacks to the Medicaid recipients they recruited.

Statement from Attorney General James on Supreme Court Allowing Access to Emergency Abortion Care in Idaho (June 27, 2024)

https://ag.ny.gov/press-release/2024/statement-attorney-general-james-supreme-court-allowing-access-emergency

The Supreme Court recently dismissed petitions for certiorari in two so-called abortion cases, allowing a preliminary injunction by the U.S. District Court for the District of Idaho to remain and with that, permitting hospitals in Idaho to continue to provide emergency abortion care pursuant to the federal Emergency Medical Treatment and Labor Act (EMTALA). AG James previously co-led a coalition of 24 attorneys general in submitting amicus briefs to the Supreme Court, the U.S. Court of Appeals for the Ninth Circuit, and the United States District Court of Idaho urging the courts to maintain access to emergency abortion care through EMTALA.

Attorney General James Announces Over $3.4 Million for the Mohawk Valley To Combat Youth Vaping Epidemic (June 21, 2024)

https://ag.ny.gov/press-release/2024/attorney-general-james-announces-over-34-million-mohawk-valley-combat-youth

AG James announced plans to distribute New York State's portion of a settlement reached with Juul Labs Inc. (JUUL) to the Mohawk Valley. The $462 million multistate settlement resolved claims related to JUUL's deceptive and misleading marketing that targeted young people and glamorized vaping. New York State will obtain $112.7 million in settlement

funds, which will be distributed across counties, Board of Cooperative Educational Services (BOCES), and the state's five largest cities. More than $3.4 million will be divided between counties and BOCES in the Mohawk Valley to fund programs aimed to reduce and prevent underage vaping.

***Attorney General James Announces Over $6.6 Million for the Capital Region To Combat Youth Vaping Epidemic* (June 21, 2024)**

https://ag.ny.gov/press-release/2024/attorney-general-james-announces-over-66-million-capital-region-combat-youth

AG James announced plans to distribute New York State's portion of a settlement reached with JUUL to the Capital Region. The $462 million multistate settlement resolved claims related to JUUL's deceptive and misleading marketing that targeted young people and glamorized vaping. New York State will obtain $112.7 million in settlement funds, which will be distributed across counties, BOCES, and the state's five largest cities. Over $6.6 million will be apportioned between counties and BOCES in the Capital Region to fund programs aimed to reduce and prevent underage vaping.

***Attorney General James Announces Over $8.8 Million for Western New York To Combat Youth Vaping Epidemic* (June 21, 2024)**

https://ag.ny.gov/press-release/2024/attorney-general-james-announces-over-88-million-western-new-york-combat-youth

AG James announced plans to distribute New York State's portion of a settlement reached with JUUL to the Western New York. The $462 million multistate settlement resolved claims related to JUUL's deceptive and misleading marketing that targeted young people and glamorized vaping. New York State will obtain $112.7 million in settlement funds, which will be distributed across counties, BOCES, and the state's five largest cities. More than $8.8 million will be split between counties and BOCES in Western New York to fund programs aimed to reduce and prevent underage vaping.

***Attorney General James Announces Over $3 Million for the North Country To Combat Youth Vaping Epidemic* (June 21, 2024)**

https://ag.ny.gov/press-release/2024/attorney-general-james-announces-over-3-million-north-country-combat-youth

AG James announced plans to distribute New York State's portion of a settlement reached with JUUL to the North Country. The $462 million multistate settlement resolved claims related to JUUL's deceptive and misleading marketing that targeted young people and glamorized vaping. New York State will obtain $112.7 million in settlement funds, which will be distributed across counties, BOCES, and the state's five largest cities. Over $3 million will be divided between counties and BOCES in the North Country to fund programs aimed to reduce and prevent underage vaping.

***Attorney General James Announces Over $4.5 Million for the Southern Tier To Combat Youth Vaping Epidemic* (June 21, 2024)**

https://ag.ny.gov/press-release/2024/attorney-general-james-announces-over-45-million-southern-tier-combat-youth

AG James announced plans to distribute New York State's portion of a settlement reached with JUUL to the Southern Tier. The $462 million multistate settlement resolved claims related to JUUL's deceptive and misleading marketing that targeted young people and glamorized vaping. New York State will obtain $112.7 million in settlement funds, which will be distributed across counties, BOCES, and the state's five largest cities. More than $4.5 million will be apportioned between counties and BOCES in the Southern Tier to fund programs aimed to reduce and prevent underage vaping.

***Attorney General James Announces Over $13 Million for the Hudson Valley To Combat Youth Vaping Epidemic* (June 21, 2024)**

https://ag.ny.gov/press-release/2024/attorney-general-james-announces-over-13-million-hudson-valley-combat-youth

AG James announced plans to distribute New York State's portion of a settlement reached with JUUL to the Hudson Valley. The $462 million multistate settlement resolved claims related to JUUL's deceptive and misleading marketing that targeted young people and glamorized vaping. New York State will obtain $112.7 million in settlement funds, which will be distributed across counties, BOCES, and the state's five largest cities. Over $13 million will be split between counties and BOCES in the Hudson Valley to fund programs aimed to reduce and prevent underage vaping.

***Attorney General James Announces Settlement With UnitedHealthcare for Failing To Provide Coverage of Birth Control* (June 20, 2024)**

https://ag.ny.gov/press-release/2024/attorney-general-james-announces-settlement-unitedhealthcare-failing-provide

AG James announced a $1 million settlement with UnitedHealthcare for failing to cover birth control under its plans, in violation of New York's Comprehensive Contraceptive Coverage Act (CCCA). The settlement followed a complaint from a Brooklyn patient denied coverage for oral contraceptives. The CCCA mandates health insurance plans cover U.S. Food and Drug Administration (FDA) approved contraceptives without copays or delays. In addition to the penalty, UnitedHealthcare will refund consumers who paid out-of-pocket for birth control and will ensure compliance with the CCCA moving forward.

***Attorney General James Announces Over $7.4 Million to the Finger Lakes Region To Combat Youth Vaping Epidemic* (June 18, 2024)**

https://ag.ny.gov/press-release/2024/attorney-general-james-announces-over-74-million-finger-lakes-region-combat

AG James announced plans to distribute New York State's portion of a settlement reached with JUUL to the Finger Lakes Region. The $462 million multistate settlement resolved claims related to JUUL's deceptive and misleading marketing that targeted young people and glamorized vaping. New York State will obtain $112.7 million in settlement funds, which will be distributed across counties, BOCES, and the state's five largest cities. More than $7.4 million will be divided between counties and BOCES in the Finger Lakes Region to fund programs aimed to reduce and prevent underage vaping.

***Attorney General James Announces Over $4.7 Million to Central New York To Combat Youth Vaping Epidemic* (June 18, 2024)**

https://ag.ny.gov/press-release/2024/attorney-general-james-announces-over-47-million-central-new-york-combat-youth

AG James announced plans to distribute New York State's portion of a settlement reached with JUUL to Central New York. The $462 million multistate settlement resolved claims related to JUUL's deceptive and misleading marketing that targeted young people and glamorized vaping. New York State will obtain $112.7 million in settlement funds, which will be distributed across counties, BOCES, and the state's five largest cities. Over $4.7 million will be apportioned between counties and BOCES in Central New York to fund programs aimed to reduce and prevent underage vaping.

***Statement From Attorney General James on Supreme Court Decision That Maintains Access to Mifepristone* (June 13, 2024)**

https://ag.ny.gov/press-release/2024/statement-attorney-general-james-supreme-court-decision-maintains-access

AG James released a statement praising the U.S. Supreme Court's decision in *FDA v. Alliance for Hippocratic Medicine*, which reversed a lower court ruling that would have restricted access to mifepristone, a drug used in medication abortions. AG James previously led a coalition of 24 attorneys general in an amicus brief supporting the FDA's approval of mifepristone as safe and effective, and emphasizing the potential harms of limiting its availability.

***Attorney General James Distributes $27.1 Million to New York City To Combat Youth Vaping Epidemic* (June 12, 2024)**

https://ag.ny.gov/press-release/2024/attorney-general-james-distributes-271-million-new-york-city-combat-youth-vaping

AG James announced plans to distribute New York State's portion of a settlement reached with JUUL. The $462 million multistate settlement resolved claims related to JUUL's deceptive and misleading marketing that targeted young people and glamorized vaping. New York State will obtain $112.7 million in settlement funds, which will be distributed across counties, BOCES, and the state's five largest cities. More than $27.1 million will be split between counties and BOCES in New York City to fund programs aimed to reduce and prevent underage vaping.

***Attorney General James Distributes $16.4 Million to Long Island To Combat Youth Vaping Epidemic* (June 12, 2024)**

https://ag.ny.gov/press-release/2024/attorney-general-james-distributes-164-million-long-island-combat-youth-vaping

AG James announced plans to distribute New York State's portion of a settlement reached with JUUL to Long Island. The $462 million multistate settlement resolved claims related to JUUL's deceptive and misleading marketing that targeted young people and glamorized vaping. New York State will obtain $112.7 million in settlement funds, which will be distributed across counties, BOCES, and the state's five largest cities. Over $16.4 million will be divided between counties and BOCES on Long Island to fund programs aimed to reduce and prevent underage vaping.

***Attorney General James Helps Secure $700 Million From Johnson & Johnson Over Products That Contained Dangerous Talcum Powder* (June 11, 2024)**

https://ag.ny.gov/press-release/2024/attorney-general-james-helps-secure-700-million-johnson-johnson-over-products

AG James, alongside a bipartisan coalition of 42 attorneys general, announced a $700 million settlement with Johnson & Johnson (J&J) for misleading consumers about the safety of baby and body powder products containing talcum powder, which have been linked to serious health risks like ovarian cancer. New York will receive $44 million as part of the settlement, which also requires J&J to stop selling talc-based products in the United States.

***Attorney General James Announces Historic Agreement With Northwell To Help More New Yorkers Receive Financial Assistance for Medical Care* (June 4, 2024)**

https://ag.ny.gov/press-release/2024/attorney-general-james-announces-historic-agreement-northwell-help-more-new

The OAG announced an agreement with Northwell Health to improve access to financial assistance for uninsured and underinsured New Yorkers. The agreement ensures individuals earning under five times the federal poverty level ($75,300 for individuals, $156,000 for a family of four) will be eligible for free or discounted care at Northwell's 21 hospitals and 56 clinics. Northwell will also reduce medical debt collection efforts and simplify financial assistance notices, providing critical relief to low-income patients.

***Attorney General James Appoints New York City Public Health Advocate Tracie M. Gardner to Opioid Settlement Board* (May 30, 2024)**

https://ag.ny.gov/press-release/2024/attorney-general-james-appoints-new-york-city-public-health-advocate-tracie-m

AG James appointed Tracie M. Gardner to the Opioid Settlement Fund Advisory Board, which is responsible for advising on the distribution of over $2.7 billion secured from opioid manufacturers and distributors. Gardner, a nationally recognized public health expert with over 30 years of experience, will focus on ensuring equitable access to treatment, especially in communities of color disproportionately affected by the opioid crisis. Gardner co-directs the National Black Harm Reduction Network and previously worked with the Legal Action Center.

***Attorney General James Secures Over $10 Million From Health Care Companies for Failing To Provide Care to New Yorkers* (May 23, 2024)**

https://ag.ny.gov/press-release/2024/attorney-general-james-secures-over-10-million-health-care-companies-failing

The OAG announced a $10.1 million settlement with RiverSpring Living Holding Corp. and ElderServe Health, Inc. for billing Medicaid for services never provided to seniors in New York City and surrounding counties. From 2012 to 2017, RiverSpring and ElderServe collected millions from Medicaid without delivering or documenting required care for members of their Managed Long Term Care Plan. The underlying case was initiated by a whistleblower under the False Claims Act, and the settlement will result in $6 million being returned to New York's Medicaid program.

***Attorney General James Applauds Decision Protecting Health Insurance Coverage for Abortion Care* (May 21, 2024)**

https://ag.ny.gov/press-release/2024/attorney-general-james-applauds-decision-protecting-health-insurance-coverage

AG James released a statement praising the New York State Court of Appeals' decision in *Roman Catholic Diocese of Albany v. Vullo*, which upheld the state's law requiring health insurers to cover abortion care. The ruling affirmed that employer-provided health insurance must include medically necessary abortion services.

New York State Office of the Medicaid Inspector General Update

Compiled by Dena M. DeFazio

OMIG-Assisted Investigation Leads to Arrests, Indictments of Orange County Medical Transportation Company Operators for Roles in $2.3 Million Medicaid Fraud Scheme – July 9, 2024

https://omig.ny.gov/news/2024/omig-assisted-investigation-leads-arrests-indictments-orange-county-medical.

OMIG Assists in Investigation that Leads to Arrest, Indictment of Medical Transportation Company Owner for Alleged $1 Million Medicaid Fraud Scheme – July 9, 2024

https://omig.ny.gov/news/2024/omig-assists-investigation-leads-arrest-indictment-medical-transportation-company-owner.

OMIG's Investigative Efforts Help Lead to Arrests, Indictments of Medicaid Transportation Operators for Roles in Medicaid Fraud Schemes – July 1, 2024

https://omig.ny.gov/news/2024/omigs-investigative-efforts-help-lead-arrests-indictments-medicaid-transportation.

Margaret M. Surowka is a former general counsel at the New York State Dental Association with over 30 years of legal experience. She routinely counsels clients facing Medicaid, Medicare, and other governmental investigations and audits as well as assists with employment and contract matters. She trains governing boards with respect to the not-for-profit law and governance issues and is a long-serving member of the Board of the National Society of Dental Practitioners. Margaret is also chair of the Hubbard Hall Center for the Arts and Education in Cambridge, N.Y.

In the Law Journals

Compiled by Jeff Ehrhardt

A Compendium of Citations to Recent Topics Published in Health Law Journals

A Hard Pill To Swallow: Privacy Implications of Direct-to-Consumer Prescription Drug Services, Varsha Challapally, 27 SMU Sci. & Tech. L. Rev. 105 (2024).

Aborted Confidentiality, Stacey A. Tovino, 65 B.C. L. Rev. 1921 (2024).

Abortion Disorientation, Greer Donley & Caroline Kelly, 74 Duke L.J. 1 (2024).

Be Careful What You Wish for: An Overreliance on Telemedicine Could Harm Health Equity, Chinelo Diké-Minor, 33 Annals Health L & Life Sci 137 (2024).

Bridging the False Certification Gap: Why "Resulting from" in the 2010 AKS Amendment Requires but-for Causation, Alexandra Wildman, 93 Fordham L Rev 359 (2024).

Corporate Takeover: A New Clash in the Old Struggle Between Corporate Rights and Public Health, John J. LoCurto, Rachel Radke, Xyruz Villariz, Jasmine Ann Castillejos, 19 J. Health & Life Sci. L. 45 (2024).

Delayed Emergency Care: How Professional Liability Insurance Affects Doctors' Decisions After Dobbs *and What Needs To Change,* Erin Stuart, 107 Marq L. Rev 1097 (2024).

Discrimination and Barriers: Abortion Access for Disabled Individuals After Dobbs, Jennifer L. Brinkley, 77 Okla. L. Rev. 53 (2024).

Evolution of the FDA Regulation of Digital Health Technologies, Ana Loloei, Allyson Mullen, 36 No. 5 Health Law. 3 (2024).

Eye for an Eye? The Sixth Circuit Loses Sight of Anti-Kickback Causation in Hathaway, Maria Russo, 65 BCL Rev 2249 (2024).

Fraud and Abuse Law: Missed Opportunities To Enhance Health Equity, Joan H. Krause, 33 Annals Health L & Life Sci 169 (2024).

From Pixels to Prescriptions: The Case for National Telehealth Licensing & AI-Enhanced Care, Fazal Khan, MD-JD, 57 Ind. L. Rev. 581 (2024).

Got Pixels? The Regulatory and Legal Implications of the Use of Third-Party Technologies on Health Care Websites, 19 J. Health & Life Sci. L. 115, Lynn Sessions and Stefanie L. Ferrari (2024).

Health Fraud From FDA Approval to CMS Payments: Why Fraud-on-the-FDA Should Be a Viable Form of Liability Under the False Claims Act, Kelly Carty Zimmerer, 62 U. Louisville L. Rev. 713 (2024).

Healthcare Fraud and Abuse: Continued Lessons Learned from High Performing Healthcare Organizations, Julie L. Agris, Ph.D., J.D., LL.M., 33 Annals Health L. & Life Sci. 101 (2024).

HHS Finalizes Amendments to HIPAA Privacy Rule To Strengthen Privacy Protections for Reproductive Health Information Post-Dobbs, Andrea Frey, Rachel Zacharias, 36 No. 5 Health L. 24 (2024).

Illusory Remedies: Why Lacking Oversight and Penalties Leave Half the Country with Only a Shadow of Healthcare, Francis Beifuss, 62 U. Louisville L. Rev. 761 (2024).

Information Privacy and Cybersecurity Responsibilities, Liabilities, Strategies, and Tactics, Jeffrey B. Miller, 70 No. 4 Prac. L. 33 (2024).

Internet Technology Companies as Evidence Intermediaries, Yan Fang, 110 Va. L. Rev. 1227 (2024)

On the Horizon: The Legalization of Physician-Assisted Suicide in Massachusetts Kligler v. Attorney General, 491 Mass. 38 (2022), Widmaier M. Charles, 105 Mass L Rev 12 (2024).

Private Law in Unregulated Spaces, Elizabeth A. Rowe, 99 NYU L. Rev. Online 249 (2024).

Recent State Legislative Attempts to Restructure Public Health Authority: The Good, the Bad, and the Way Forward, Darlene Huang Briggs, Elizabeth Platt, Leslie Zellers, 52 J.L. Med. & Ethics 43 (2024).

Regulating Digital Health Care for the Cognitively Impaired, Kathryn Huber, Tara Sklar 19 J. Health & Life Sci. L. 97 (2024).

Regulating the Psychedelic Renaissance: FDA's Critical Role in the Push for Scheduling Reform To Expand Research into Psychedelic Medicines, Saumya Sinha, 76 Admin. L. Rev. 731 (2024).

State Telemedicine Abortion Restrictions and the Dormant Commerce Clause, Laura Hu, 91 U Chi L. Rev 1411 (2024).

Telehealth in Reproductive Health Care: A New Frontier in the Fight for Abortion Access, Katie Corwin, 27 CUNY L. Rev. 304 (2024).

The Care Bureaucracy, Yiran Zhang, 99 Ind. L.J. 1241 (2024).

The Challenge for Coronavirus Vaccine Testing, Bastian Steuwer, 28 J. Ethics & Soc. Phil. 30 (2024).

The Changing Nature of Medical Records in the 21st Century, Samuel D. Hodge, Jr., 70 No. 4 Prac. L. 38 (2024).

The Missing Puzzle Piece: Using Health Data To Close the Social Determinants of Health Gap, Melissa A. Soliz, Eric Setterlund, Annie Harrington, Sarah Y. Raybin, 19 J. Health & Life Sci. L. 3 (2024).

The Paradox of the Three Wise Monkeys: Discovery and Disclosure of Information Regarding Dangerous Health Care Providers, John Zen Jackson & Madeline B. Gayle, 30 Widener L. Rev. 103 (2024).

The Private Rights Model of Qui Tam, Sarah Leitner, 76 Fla. L. Rev. 865 (2024).

The Use of Mediation to Reduce Medical Malpractice Claims, Unnecessary Antimicrobial Therapy, and Resistance Rates in Patients Across the Nation, Shifra Ben-Jacob, 25 Cardozo J Conflict Resol 533 (2024).

United We Fall? The Change Healthcare Cyberattack and the Danger of a Too-Big-to-Fail Health Insurer, Brendan Williams, 101 Denv. L. Rev. Forum 1 (2024).

Using Jewish Law: Jewish Religious Liberty Advocacy for the Right to Abortion, Michael A. Helfand, 70 Wayne L. Rev. 51 (2024)

When FDA Comes Knocking and What To Do About it: FDA Regulatory and Enforcement Risks Relevant to Academic Medical Centers, Health Systems, and Research Institutions, Beth P. Weinman, David Peloquin, Sarah Blankstein, Stephen D. Sencer, 19 J. Health & Life Sci. L. 134, (2024).

Wind-Downs and Whistleblowers: Navigating Qui Tam in Bankruptcy, Earl M. Forte & Michael Barber, 43-AUG Am. Bankr. Inst. J. 24 (2024).

Jeff Ehrhardt is an associate in the Health Services and Commercial Litigation practice groups at Rivkin Radler LLP.

For Your Information

By Claudia O. Torrey

A Few Informational Highlights

*The theme for this Journal is digital health, which begs the question, What is Digital Health? According to "Continuum" of CareCloud.com, digital health and/or digital healthcare (DH) refers to a broad multidisciplinary concept reflecting the intersection of technology and healthcare. DH necessarily includes wearable technology, telemedicine, mobile health (mHealth) apps, electronic medical records, and electronic health records.[1]

*The World Health Organization has a global strategy on digital health for the years 2020-2025.[2] The purpose of this global strategy is to promote healthy lives and well-being for people everywhere of all ages, via technological products that assist people locally, regionally, and/or nationally. As of February 20, 2024, the Global Initiative on Digital Health (GIDH) mission statement seeks to foster improved alignment in the digital health sector providing governments and partners tools, building blocks, and platforms as needed for sustainable health system digitalization.[3] The GIDH also seeks to support the aforementioned global strategy.

*In a recent 2024 report,[4] The Commonwealth Fund reports that the United States ranks last among comparable industrialized countries regarding access, outcomes, and administrative efficiency; thus the United States seems to spend the most on health care while receiving the least for its investment.[5] One report bright spot appears to be efforts in prevention, safety, and patient engagement.[6] One could perhaps argue that more utilization of digital health could potentially increase both health access and outcomes, while lowering health costs.

*Electronic health record vendors Epic and Oracle Health have recently "signed on" to a United States Department of Veteran Affairs (VA) Interoperability Pledge.[7] The goal of the pledge is to boost information exchange between VA facilities and participating health systems, thereby improving care coordination for veterans receiving care at both the VA and within their communities.[8] Some of the health systems that are a part of this pledge include Kaiser Permanente, Emory Healthcare, Mass General Brighham, and Tufts Medicine.[9] Thus, Epic and Oracle are promising that all of their hospital clients will be able to connect to VA systems for more efficient data sharing.[10]

*The title of the 2024 keynote address at the Healthcare Information and Management Systems Society Meeting was "Smart Hospital Revolution: Redefining Patient Care with Technology."[11] Leaders from Samsung Electronics explored the concepts of digital health tools, robotics, and other innovative technologies for healthcare.

Claudia O. Torrey is a Charter Member of the Health Law Section.

Endnotes

1. https://www.carecloud.com/continuum.
2. Digital Health, World Health Organization (last accessed Nov. 15, 2024), https://www.who.int/health-topics/digital-health#tab=tab_1.
3. Global Initiative on Digital Health, World Health Organization (last accessed Nov. 15, 2024), https://www.who.int/initiatives/gidh.
4. David Blumenthal, Evan D. Gumas, Arnav Shah, Munira Z. Gunja, Reginald D. Williams II, *Mirror, Mirror 2024: A Portrait of the Failing U.S. Health System,* The Commonwealth Fund, https://www.commonwealthfund.org/publications/fund-reports/2024/sep/mirror-mirror-2024.
5. *Id.*
6. *Id.*
7. Mike Miliard, *Epic and Oracle Health Sign on to Veteran Interoperability Pledge*, Healthcare IT News (Sept. 19, 2024), https://www.healthcareitnews.com/news/epic-and-oracle-health-sign-veteran-interoperability-pledge.
8. *Id.*
9. *Id.*
10. *Id.*
11. *HIMSS24 APAC: Leading Voices in Digital Health Converge in Seoul*, Healthcare Information and Management Systems Society, Inc. (June 26, 2024), https://gkc.himss.org/news/himss24-apac-leading-voices-digital-health-converge-seoul,

In the New York State Courts

By Dayna B. Tann and Marc A. Sittenreich

First Department Rules That Health Care Providers Must Offer Conclusive Evidence That the Plaintiff's Care Was Specifically Impacted by Their Response to the COVID-19 Pandemic in Order To Assert Immunity Under the EDPTA on a Motion To Dismiss

Holder v. Jacob, 216 N.Y.S.3d 134 (1st Dep't 2024)

In March 2020, in response to COVID-19's impact on the operation of New York State's health care facilities, the governor issued numerous executive orders modifying or suspending various provisions of law to facilitate the state's collective response to the disaster. Among them was Executive Order 202.10, issued March 23, 2020, which temporarily modified or suspended several provisions of the Education Law and granted health care providers "immun[ity] from civil liability for any injury or death alleged to have been sustained directly as a result of an act or omission by such medical professional in the course of providing medical services in support of the State's response to the COVID-19 outbreak."

Subsequently, the New York State Legislature enacted the Emergency or Disaster Treatment Protection Act (EDPTA), which afforded immunity from civil and criminal liability to health care facilities and professionals that might have resulted from treatment of individuals during the COVID-19 emergency. The version of the statute in effect at the time relevant to this action set forth the following three elements a medical provider must show to demonstrate entitlement to immunity: (a) the facility or professional was "arranging for or providing health care services pursuant to a COVID-19 emergency rule or otherwise in accordance with applicable law"; (b) the "act or omission occur[red] in the course of arranging for or providing health care services" and the patient's treatment is "impacted" by the provider's "decisions or activities in response to or as a result of the COVID-19 outbreak and in support of the state's directives"; and (c) the facility or professional is "arranging for or providing health care services in good faith."

Plaintiff is a patient who fell and sustained a brain hemorrhage while being treated at Montefiore Medical Center in April 2020. He brought a medical malpractice action against the hospital, two of its physicians, and one of its nurses in the Supreme Court of the State of New York, County of Bronx. Defendants moved to dismiss, arguing that they were immune from liability under the EDPTA and Executive Order 202.10. In support of their motion, defendants filed over 7,000 pages of medical records, affidavits from each defendant provider, and an affidavit from the hospital's chief quality officer and vice president, which described the numerous operational strains the COVID-19 virus had inflicted on the hospital.

The Supreme Court denied defendants' motion, finding that they had not conclusively established their defense insofar as they failed to demonstrate that the pandemic affected plaintiff's treatment "such that his condition could not be properly diagnosed and promptly treated," or that the alleged departures in medical care "were the result of a direct impact from defendants' response to the pandemic." Defendants appealed.

The First Department observed that a CPLR 3211(a)(7) motion is typically focused strictly on the sufficiency of the facts in the pleadings. Because defendants submitted affidavits and other evidentiary materials, the court's focus was "no longer merely on the adequacy of the complaint's allegations," and the "evidence [submitted] must conclusively establish a defense to plaintiff's claims as a matter of law." In other words, the court's inquiry changed "from whether the pleader has *stated* a cause of action to whether the pleader *has* a cause of action amenable to relief."

The First Department held that, of the three conditions imposed by the EDPTA, there was "no question that the defendants were arranging for or providing health care services as per the statute, and were doing so in good faith." Accordingly, the court needed to consider only whether defendants conclusively established the second condition for immunity under the statute: whether "the treatment of [Plaintiff was] impacted by [Defendants'] decision or activities in response to or as a result of the COVID-19 outbreak."

The court asserted that a "statute conferring immunity must be strictly construed" and "the applicability of the defense, itself, requires a fact-intensive inquiry." While the court noted other defendants had made the requisite showing on a motion to dismiss, it found that defendants' evidentiary submission – which "described numerous and pervasive systemic changes to hospital operation and patient care occasioned by the pandemic" – merely "suggested" that plaintiff's treatment was impacted by the hospital's response to the COVID-19 outbreak, but did not conclusively prove such impact, as re-

quired under CPLR 3211(a)(7). The court noted that "only minimal discovery had been conducted at the time the motion was made," and thus it was "premature" for the court to determine whether defendants were entitled to immunity.

Lastly, the court rejected defendants' argument that Executive Order 202.10 provided an independent basis for complete immunity warranting dismissal of the complaint. The court observed that "several courts" had concluded that "the EDTPA was a codification of the immunity contained in Executive Order 202.10" and thus "the Executive Order was 'subsumed' into the EDPTA." While the First Department did not expressly adopt that theory, it held that defendants could not succeed on their immunity argument under Executive Order 202.10 because they "had not established entitlement to such immunity under the EDTPA."

District Court Greenlights New York City Administrative Scheme Authorizing the Sheriff To Issue Pre-Hearing Sealing Orders Against Businesses Found To Be Selling Cannabis Without a License

Moon Rocket Inc. v. City of New York, No. 24 Civ. 4519, 2024 WL 3454901 (S.D.N.Y. Jul. 18, 2024)

In March 2021, the New York State Legislature legalized and regulated adult-use cannabis by enacting the Marihuana Regulation and Taxation Act (the MRTA or the "Cannabis Law"). On April 20, 2024, the Legislature amended the MRTA and added § § 7-551 and 7-552 to New York City's Administrative Code (the "NYC Admin. Code"), empowering the Office of the City Sheriff to inspect, issue summonses to, and seal the premises of businesses that it finds to be selling cannabis without a license.

Plaintiffs are 27 businesses subject to sealing orders issued by the sheriff under this enforcement scheme. They filed suit under 42 U.S.C. § 1983 against the city and various city officials in the United States District Court for the Southern District of New York, alleging a deprivation of their 14th Amendment procedural due process rights. Plaintiff moved for a preliminary injunction prohibiting the city from enforcing N.Y.C. Admin. Code § § 7-551 and 7-552 and allowing their businesses to reopen pending the outcome of their lawsuit.

The District Court began its decision on plaintiffs' preliminary injunction motion with an overview of the enforcement scheme. Under NYC Admin. Code § 7-551, the sheriff can "issue and execute an order to seal a premises where any business is engaged in conduct prohibited by [the Cannabis Law] and which poses an imminent threat to public health, safety, and welfare." Pursuant to Cannabis Law § 138-b(6), a sealing order may be issued only where the "unlicensed activity is 'more than a *de minimis* part of the business activity on the premises or in the building to be sealed.'" Within five days after a sealing order is issued, the business is entitled to a hearing before the New York City Office of Administrative Trials and Hearings (OATH), which submits a recommendation to the sheriff's office as to whether the order was properly granted. Within four days of the recommendation, the sheriff's office must decide whether the order will be lifted or remain in place for one year or until the business submits sufficient evidence that the unlicensed activity has been abated. The sheriff's final determination is subject to review before the New York State Supreme Court under CPLR Article 78.

The District Court then addressed plaintiffs' procedural due process challenge and concluded that they were unlikely to succeed on the merits. While it was undisputed that plaintiffs had a "property interest in their ability to operate their businesses other than the unlicensed sale of cannabis" – and the "general rule" is that "a party cannot invoke the power of the state to seize a person's property without a prior judicial determination that the seizure is justified" – the court found sufficient process was afforded to businesses to contest the sealing orders before a final decision is made.

To determine whether "the demands of the Due Process Cause are satisfied" despite the state's "possession of property before final judgment is rendered," the District Court turned to the three-factor test articulated by the Supreme Court in *Matthews v. Eldridge*, 424 U.S. 319, 335 (1976). The court found that the first factor – "the private interest that will be affected by the official action" – weighed in favor of plaintiffs, as they had a significant interest in operating their businesses for purposes other than the unlicensed sale of cannabis. However, the court found that the second *Mathews* second factor – "the risk of an erroneous deprivation of such interest through the procedures used" – weighed in favor of the city, as it found this risk to be low. In addition to the fact that the sheriff must determine both that the business engaged in the unlicensed sale of cannabis and that it poses an imminent threat to the public health, safety, and welfare, the court explained that the "OATH hearings provide a meaningful opportunity to be heard to challenge sealing orders issued in error," including the ability to be represented by counsel, present evidence, and cross-examine the officer who issued the order. The court noted that the whole administrative "process lasts approximately nine days," after which the businesses can seek judicial review – including a preliminary injunction – in state Supreme Court. Lastly, the court found that the third *Mathews* factor – "the Government's interest" – weighed in favor of the city, as it has a "manifestly important and urgent interest in closing the unlicensed cannabis shops that pose immediate risk to the public."

In light of "the low risk of erroneous deprivation and the substantial government interest in protecting public safety," the District Court concluded that N.Y.C. Admin. Code § § 7-551 and 7-552 "provide adequate procedural protections to guarantee plaintiffs' due process rights under the 14th Amendment." Because it found that plaintiffs were unlikely to succeed on the merits, it denied their motion for a preliminary injunction.

Eastern District of New York Holds That There Is No Private Right of Action To Seek Reimbursement for COVID-19 Testing Under the CARES Act and the FFCRA

Biodiagnostic Labs, Inc. v. Aetna Health Inc. (New York), No. 23 Civ. 9570, 2024 WL 3106169 (E.D.N.Y. June 23, 2024)

Plaintiff, a medical testing laboratory, brought eight separate actions against various health insurers (collectively, "defendants") in the United States District Court for the Eastern District of New York, seeking full or partial payment for COVID-19 tests it conducted on behalf of defendants and their affiliates' insureds. All defendants moved to dismiss on similar grounds, prompting the court to consolidate the cases for decision on defendants' motions.

Plaintiff is out-of-network with all of defendants' health plans. Between the onset of the COVID-19 pandemic and May 2023, plaintiff provided thousands of COVID tests to defendants' insureds. Patients assigned their right to insurance coverage for the tests to plaintiff, who in turn submitted claims for out-of-network reimbursement to defendants. Defendants reimbursed many of plaintiffs' claims at the rates posted on plaintiff's website. On other claims, however, defendants did not pay anything or did not pay in full. In all eight lawsuits, plaintiff sought additional reimbursement on those allegedly unpaid and underpaid claims.

In each lawsuit, plaintiff's Fourth Cause of Action asserted a right to payment under the Coronavirus Aid, Relief, and Economic Security Act (the "CARES Act") and its companion statute, the Families First Coronavirus Response Act (FFCRA). Under the CARES Act, health insurers must reimburse out-of-network diagnostic tests "in an amount that equals the cash price for such service as listed by the provider on a public internet website." Defendants moved to dismiss this claim, arguing the statute does not create a private right of action and may only be enforced by the appropriate federal agencies. The court agreed.

Surveying decisions from similar cases in various federal courts across the country, the court observed that "[i]n every instance, the courts, including the Ninth Circuit (the only Court of Appeals to have considered the issue), have dismissed [such suits] on the ground that there is neither an express nor

implied private right of action under the CARES Act." The court placed particular emphasis on the Ninth Circuit's decision in *Saloojas, Inc. v. Aetna Health of California, Inc.*, 80 F.4th 1011, 1016 (9th Cir. 2023), which noted that for decades the Supreme Court has been hesitant to find an implied private right of action where Congress did not expressly create one. The court was equally swayed by the fact that both the CARES Act and the FFCRA vested enforcement power in various federal agencies, namely the secretaries of health and human services, labor, and the treasury. Citing *Saloojas*, the court found the "fact that these provisions provide an enforcement mechanism but only through the Secretaries suggests a lack of congressional intent to create a private right of action for providers."

The court also rejected plaintiff's effort to create "a false determination of congressional intent" by counting itself among the "class" for whose benefit the statute was enacted simply because the CARES Act requires insureds to pay its posted rates. In doing so, the court found that "the obvious purpose of this provision of the CARES Act was to encourage patients . . . to get tested by relieving them of financial concern that might deter them from obtaining such testing." In the court's view, plaintiff was, at most, a "collateral beneficiary" of the statute, because there was "no crisis in the laboratory testing industry that Congress sought to remedy by passing" it. Thus, the court dismissed plaintiff's CARES Act claims.

The court then turned to plaintiff's three "breach of contract" claims – two of which, it noted, were actually equitable in nature. To the extent these claims arose under ERISA-governed health plans, the court agreed with defendants that all three were preempted, and that plaintiff was bound by the resolution procedures set forth in ERISA or in the plans themselves. On this issue, the court noted that the relevant provisions of both the CARES Act and the FFCRA incorporate ERISA when they are applied to ERISA-governed plans, and that the statutory "requirement of COVID-19 testing cov-

erage is [therefore] intended to interlock with ERISA." The court's finding was supported by reference to both *Saloojas* and decisions from various federal district courts in New Jersey, Minnesota, and California.

Finally, the court confronted the claims arising under non-ERISA plans. But first, the court remarked that "no one, at least for purposes of these motions, seems to know" which claims fall under ERISA plans and which do not. The court rejected defendants' attempt to saddle plaintiff with the burden of "separately plead[ing] claims that fall under non-ERISA governed policies," because defendants have ready access to the relevant plan documents and are better-positioned to make this determination. Yet, this missing information was of no moment, because the court – having dismissed the ERISA-based claims at the pleading stage – found no basis to exercise supplemental jurisdiction over the non-ERISA claims. Indeed, the court held that the non-ERISA claims are simple, state-law breach of contract claims, and that merely incorporating the CARES Act's "pricing mechanism" was insufficient to confer federal jurisdiction. Because "any reference to the CARES Act will be only to measure what damages plaintiff is owed," the non-ERISA claims would have "no substantial impact on federal law" and therefore belonged in state court.

Court Dismisses Physician's Discrimination Claims for Failure To Exhaust Her Administrative Remedies With the Public Health and Health Planning Council

Joseph v. NYU Grossman School of Medicine, No. 650521/2024, 2024 WL 4068660 (Sup. Ct., N.Y. County Sept. 5, 2024)

Plaintiff, the former chief of trauma and acute care surgery at NYU Langone Hospital, filed suit in the Supreme Court of the State of New York, County of New York against the hospital and various individuals under the New York State Human Rights Law (NYSHRL). Plaintiff claimed that she was subjected to discrimination due to her race and gender, purportedly resulting in her demotion, restrictions being placed on her hospital privileges, and the termination of her employment. Plaintiff also contended that the hospital's report to the National Practitioner Data Bank (NPDB) concerning the restriction on her hospital privileges was defamatory.

Plaintiff alleged that during her employment, she was treated disparately from her male colleagues and witnessed "rampant misogyny and racism" from hospital staff. Plaintiff contends that the hospital purportedly demoted her, without notice or cause, while promoting less qualified white male doctors. According to plaintiff, the hospital suspended and restricted her privileges without just cause, based on surgical complications for which similarly situated male colleagues did not lose hospital privileges, and submitted a false report to the NPDB regarding the hospital's concerns about her character and honesty. Plaintiff disputed the restrictions on her clinical privileges and requested an administrative hospital hearing. That hearing was still ongoing when plaintiff commenced her suit. Plaintiff claimed her employment was subsequently terminated after she refused to resign.

Defendants moved to dismiss the complaint. They argued, among other things, that the court lacked subject matter jurisdiction over plaintiff's claims because of her failure to comply with the administrative grievance procedure required by Public Health Law (PHL) § 2801-b.

The court reviewed the statutory procedure under which a physician may challenge a termination of hospital privileges and observed that such procedure requires a physician to first file a complaint with the Public Health and Health Planning Council (PHHPC) for review. Only after PHHPC review is exhausted may the physician seek redress in court. The court noted that where a physician asserts claims based on a hospital's allegedly wrongful withdrawal of staff privileges, regardless of whether such claims seek damages or reinstatement, the court lacks subject matter jurisdiction to entertain them until the claims have been reviewed by the PHHPC under the procedure provided by PHL § 2801-b.

Plaintiff argued that her complaint was not subject to dismissal, as it sought to redress the discrimination to which she was allegedly subjected, rather than challenge the termination of her privileges and reinstatement of her hospital privileges. However, the court determined that because plaintiff's claims arose from, among other things, the restriction of her hospital privileges, and plaintiff had not yet exhausted her administrative remedies with the PHPPC, it did not have subject matter jurisdiction over her claims. The court found that it could not extrapolate the restriction of plaintiff's hospital privileges from her complaint, because to do so would leave the complaint devoid of actionable injury. In other words, the court held that the restriction of plaintiff's privileges was "inextricably linked" to the alleged wrongful demotion and termination.

Finally, the court dismissed plaintiff's defamation claim. The court found that the alleged defamatory statements – concerning the hospital's concerns over plaintiff's "character" and "honesty" – constituted non-actionable opinion.

(Editors' Note: Garfunkel Wild, P.C. represented the defendants in the *Joseph* action.)

Second Circuit Finds State Law Claims Based on Plan Administrator's Promise of Payment to Out-of-Network Provider Preempted by ERISA Where the Administrator Simply Relayed Terms of the Applicable Health Plan

Park Ave. Podiatric Care, P.L.L.C. v. Cigna Health & Life Ins. Co., No. 23-1134, 2024 WL 2813721 (2d Cir. June 3, 2024)

Plaintiff is a New York-based health care provider that does not participate in the provider network maintained by Cigna Health Life Insurance Company ("Cigna"). In 2019, plaintiff performed various foot surgeries on "SS," a beneficiary of an employee health plan administered by Cigna. Before performing those surgeries, plaintiff contacted Cigna by telephone to inquire about the payment it would receive as an out-of-network provider. Cigna informed plaintiff that "payment for covered services rendered to SS was based upon 80 percent of the customary rate." Plaintiff billed Cigna $197,350 for the surgeries but was paid only $7,199, far less than the amount purportedly promised.

Plaintiff brought an action against Cigna in the United States District Court for the Southern District of New York, asserting state law claims for breach of contract, unjust enrichment, promissory estoppel, and violation of New York's Prompt Pay Law. Cigna moved to dismiss the complaint on the ground that plaintiff's state law claims are preempted by the Employee Retirement Income Security Act of 1974 (ERISA), which governs SS's health plan. The District Court granted Cigna's motion, and plaintiff appealed.

The Second Circuit observed that ERISA has an express preemption provision, under § 514(a), which specifies that the statute "supersedes or preempts all state laws insofar as they 'relate to any employee benefit plan.'" The Supreme Court has interpreted § 514(a) to "preempt[] state common law claims that seek to rectify 'alleged improper processing of a claim for benefits under' ERISA-regulated plans." Claims "relate to" an ERISA-governed plan where they have "a connection with or reference to" an ERISA plan or where the "existence" of an ERISA plan "is a critical factor in establishing liability."

Plaintiff's primary argument, on appeal, was that the District Court improperly found its claims preempted because they were "not related to an ERISA-governed plan." Plaintiff contended that its claims were based a "separate legal duty that arose from the commitment Cigna made . . . during the pre-surgery phone calls" to provide reimbursement "based on the industry's customary rate."

The Second Circuit rejected this argument, finding that plaintiff's own pleading made clear that Cigna merely "communicated the terms of SS's out-of-network coverage under SS's employee health plan," and did not make any independent promise of payment. First, plaintiff alleged that when the plan provides out-of-network benefits, "Cigna determines the amount Cigna will allow for a covered service to an out-of-network provider." Thus, plaintiff "understood," during the pre-surgery calls, that "the extent of Cigna's obligations to [it] would be defined by the plan's terms." Second, plaintiff alleged that Cigna represented the rate of reimbursement for "covered services rendered to SS," and not the rate it would pay for the specific services in question. The court found the term "covered services" to signal that "any duty Cigna had to pay" plaintiff "was based on Cigna's obligations as claims administrator for SS's plan."

Alternatively, plaintiff contended that the District Court should not have considered an excerpt from SS's Summary Plan Description – which demonstrated the plan is governed by ERISA – because that document was not attached to or expressly incorporated by reference into the complaint. The Second Circuit rejected this argument as a well, as plaintiff's complaint "presupposes the existence of a relationship between Cigna and SS though a health insurance plan," and because the threshold questions of "whether SS's plan was an ERISA-regulated plan" and whether plaintiff "was the recipient of any duty" thereunder were "necessary to resolve" at the pleading stage.

Dayna B. Tann and **Marc A. Sittenreich** are partners at Garfunkel Wild, P.C., a full-service health care law firm representing hospitals, health systems, physician groups, individual providers, nursing homes, and other health-related businesses and organizations. Both Tann and Sittenreich are members of the firm's litigation practice group. Their respective practices focus on general commercial and health care litigation and arbitration, including breach of contract and business tort claims, payer-provider reimbursement disputes, employment actions, disability discrimination and accommodation claims, dissolution proceedings, and physician practice disputes.

Digital Health Applications: Use Cases and Regulatory Overview

By Emma Carey, Michael Purcell, and Jonathan Walland

I. Introduction

Digital health technologies (DHTs) refer to a broad universe of transformative technologies that hold the promise of revolutionizing the way individuals access and manage their health care. The U.S. Food and Drug Administration (FDA) has offered a broad definition of the term that captures just how varied the uses of such technologies can be:

> Digital health technologies use computing platforms, connectivity, software, and sensors for health care and related uses. These technologies span a wide range of uses, from applications in general wellness to applications as a medical device. They include technologies intended for use as a medical product, in a medical product, as companion diagnostics, or as an adjunct to other medical products (devices, drugs, and biologics). They may also be used to develop or study medical products.[1]

While industry efforts to increase the development and uptake of digital health technologies DHTs predates the COVID-19 pandemic, the need for novel solutions to facilitate the provision of health care during the public health emergency drastically increased the pace of innovation and the recognition by regulators of the unique benefits that such technologies can provide. Regulators have freely acknowledged the various benefits of expanded DHT use, including the potential to increase access to care and convenience for patients – particularly for vulnerable patient populations like those in low-income and rural locations, as well as those experiencing infectious diseases or suffering from weakened immune systems

Individuals who reside in low-income communities often face various deleterious social determinants of health, which are non-medical factors that can negatively influence health outcomes. Some examples of social determinants of health include income and social protection, unemployment and job insecurity, working life conditions, food insecurity, housing, basic amenities and the environment, and access to affordable health services of decent quality. These adverse social determinants can make it difficult for patients to attend doctors' appointments due to lack of transportation, inability to take time off work, or the impact of disabilities. DHTs hold the promise to reduce or eliminate some of these barriers by allowing patients to attend their medical appointments electronically in the comfort of their own home or office. Individuals who reside in rural communities often have similar impediments to health care. According to a recent study by University of Pennsylvania's Wharton Health Care Management Alumni Association:

> Compared with urban populations, rural residents generally have higher poverty rates, a larger elderly population, tend to be in poorer health, and have higher uninsured rates than urban areas. At the same time, rural areas often have fewer physician practices, hospitals, and other health delivery resources. These socioeconomic and health care challenges place rural populations at a disadvantage for receiving safe, timely, effective, equitable, and patient-centered care.[2]

Beyond rural and low-income populations, other vulnerable patient populations like patients with infectious diseases, weakened immune systems, or other health issues making in-person care provision more dangerous may similarly benefit from the increased use of DHTs.

Another meaningful benefit that DHTs promise is the opportunity to maximize efficiencies for health care providers (HCPs).[3] Various DHTs offer opportunities to minimize day-to-day workload for HCPs by, among other things, increasing the ease of real-world data collection, offering platforms for virtual visits that allow HCPs to see more patients in a day, and streamlining the integration of data into electronic patient charts and minimizing the need for providers to spend time on clerical or administrative tasks.

Given these wide-ranging benefits, regulators like FDA, the Centers for Medicare & Medicaid Services (CMS), the U.S. Department of Health and Human Services (HHS) have sought to promote the development and use of these technologies by, among other things, seeking in put on how to establish more flexible regulatory frameworks to permit their use[4] and establishing programs aimed at fostering further innovation in this space.[5] However, DHT use in the health care space is not only forward-looking. From internet-enabled diagnostic medical devices to electronic health record (EHR) systems to telehealth, many digital technologies are already being deployed in the health care field. This article provides a discussion of current clinical uses of digital health in hos-

pitals, clinics, and other traditional patient care models, and explores the relevant laws that govern their development, approval, and use. It also discusses ongoing challenges facing DHT developers, HCPs, patients, payors, and other industry actors in their efforts to continue expanding the use of DHTs in patient care.

II. Regulation of DHTs

DHTs are regulated by various government agencies at both the federal and state[6] level. At the federal level, FDA, CMS, the HHS Office for Civil Rights (HHS-OCR), and the Federal Trade Commission (FTC) are among the regulators with the most significant enforcement authority over certain types of DHTs. Collectively, these agencies have established frameworks for regulating DHTs throughout their product lifecycles that are aimed at facilitating the safe and effective development, manufacture, commercialization, distribution, and use of DHTs within the health care industry. These regulators have aimed to assist DHT developers and manufacturers in understanding and assessing vital questions throughout the development and commercialization processes, including, among other things, the threshold question of whether the commercialization of a DHT is legally permissible under existing regulatory frameworks and, assuming so, what technical, operational, and validation requirements will apply; how government and private insurance payors will impact payment of new DHTs; and whether provision of such technologies may raise questions under anti-fraud and inducement laws, such as the Anti-Kickback Statute.[7]

A. FDA Regulation

Under the federal Food, Drug, and Cosmetic Act of 1938 (FDCA) and its implementing regulations, FDA's Center for Devices and Radiological Health (CDRH) has the authority to regulate firms who develop, manufacture, repackage, relabel, and/or import medical devices within the United States.[8]

1. Scope of FDA Authority Over DHTs

The FDCA defines a medical device as:

> an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is . . . [among other things] intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or intended to affect the structure or any function of the body of man or other animals.[9]

In 2016, as part of the 21st Century Cures Act, Congress clarified the scope of DHTs that qualify as medical devices, specifically excepting certain categories of commonly used low-risk DHTs from the medical device definition.[10]

Under the FDCA's definition, whether and when a product is considered a "medical device" and is therefore subject to regulation by FDA turns in large part on the intended use of the product; intended use can be established by, among other things, the design, function, and capabilities of the product; the circumstances surrounding its distribution; and any express or implied statements made by its developer, manufacturer, or distributor.[11] This means that a DHT that includes a diagnostic algorithm intended to interprets electrocardiograms would likely be considered an FDA-regulated medical device, whereas a direct-to-consumer app that recommends eating more fruits and vegetables to improve overall health would not. Less intuitively, however, the variety of considerations impacting a product's intended use means that it is possible that two products with the same functionalities may be classified differently – one as a medical device and one as a non-medical device – if evidence indicates that they are intended for different uses. For example, a wearable device that measures the pulse rate of users may be a medical device if it is intended to be used by patients with cardiovascular disease to collect data, monitor health status, or inform the provision of care, but might not qualify as a medical device if it provides less specific data to the user and is only marketed for monitoring the user's pulse rate during exercise because such a use is not related to a specific health purpose.

Given the complexity inherent in assessing whether a DHT falls within the definition of medical device – including

whether it falls within a statutory exception – FDA has issued numerous policy guidance documents to aid DHT developers and manufacturers in undertaking such assessments.[12] If a DHT is not a medical device, it falls outside of the scope of FDA's regulatory authority. FDA has also announced its intention to engage in a policy of enforcement discretion (i.e., to not enforce requirements under the FDCA) for certain low-risk DHTs that may qualify as medical devices under the FDCA, including certain software to facilitate telemedicine, certain functions that perform simple calculations routinely used in clinical practice, and certain "coaching" software functions that help patients self-manage their health.[13]

FDA has also established various resources, including the Digital Health Center of Excellence,[14] to provide additional advice and guidance for industry throughout the development, commercialization, and use of DHTs.

2. Medical Device Regulatory Framework

When any product, including a DHT, meets the definition of a medical device, it becomes subject to the regulation and oversight of FDA's CDRH. FDA regulations establish requirements that apply throughout the medical device product lifecycle including, but not limited to, premarket notification or approval, and product design, development, clinical validation, and quality management requirements.[15] Which FDA requirements apply to a given medical device depends on such device's level of risk and attendant classification.

CDRH categorizes medical devices into Class I, II, or III classifications, based on their level of risk.[16] Class I devices are those that present the lowest risk of illness or injury, while Class II covers moderate-risk tools. Both Class I and II are subject to a less burdensome regulatory process, with the focus on registration, manufacturing and labelling.[17] In contrast, Class III devices will typically necessitate generation of pre-clinical and clinical data to support a formal approval. A notable exception exists for Class III devices that can demonstrate safety and efficacy by proving substantial equivalence to existing "predicate devices."[18] In other cases, a de novo device can be approved without needing to identify a predicate device, based on FDA's determination that reasonable assurances of safety and effectiveness can be provided by general or special controls.[19] But the Premarket Notification pathway, often referred as 510(k) clearance, in reference to its section in the Food, Drug and Cosmetic Act – is often unavailable to novel digital health tools that consist of new innovative technology, for which there are no precedents and reliance on general or special controls is insufficient. This sometimes leads to a related pitfall where digital health developers are tempted to 'chase the approval' by reducing the functionality of a digital health tool in order to qualify as a Class I or Class II device. Limited function digital health tools may prove unappealing to patients and providers, and therefore commercially unviable.

Similarly, inexperienced developers are sometimes tempted to seek the easiest and quickest approval pathway, but might later find that their chosen pathway is rejected by CDRH based on the product risk profile, or while adequate for FDA purposes, is insufficient to generate the efficacy and quality data needed to support CMS or private payer reimbursement decisions. The software and technology start-up strategy of developing a "minimum viable product" – a bare-bones version with limited features and functionality, intended to provide proof of concept and solicit beta tester feedback – often doesn't work in the highly regulated health care field.

B. FTC Regulation

While the FDA's role in regulation of DHTs is limited to those that meet the definition of medical devices, the FTC regulates a broader universe of DHTs, sharing jurisdiction over medical device DHTs and also wielding regulatory authority over DHTs that do not meet the definition of medical device. However, the FTC's scope of regulatory authority is more narrow than FDA's, as it is focused on preventing "unfair or deceptive acts or practices,"[20] in large part as it relates to product advertising. In terms of digital health, the FTC's responsibility has grown in recent years, particularly in the area of direct-to-consumer (DTC) health apps and tools, which often fall outside the ambit of HIPAA regulation. FTC has stepped up to fill this void by aggressively regulating DTC DHTs to promote consumer protection by ensuring that product claims and advertisement is not deceptive or misleading to patients.

C. CMS Regulation

CMS' role in digital health is complex and often relies on its function as a significant payor in the U.S. health care market. CMS' efforts to promote equity in the health care system through promotion of digital health rely on various regulatory approaches, including the "stick" of CMS program rules and the "carrot" of CMS funding incentives and reimbursement to support digital health initiatives and pilot programs. Outside of Medicare/Medicaid funding, CMS is also bridging the digital health care gap among those beneficiaries with low digital literacy and in lower-income regions. A stated goal of CMS' 2024 Medicare Advantage program is to "develop and maintain procedures to identify and offer digital health education to enrollees with low digital health literacy to assist with accessing any medically necessary covered telehealth benefits."[21]

CMS' role is vital to the successful uptake of DHTs, as a key barrier to their expanded use is the difficult process of negotiating with CMS and private insurance companies for reimbursement for each new digital health product. While

some DHT developers have successfully obtained CMS reimbursement by going through the lengthy process of seeking a new billing code and then obtaining a national coverage decision, many have been discouraged. Historically, new DHTs have needed to qualify under an existing benefit category, which can include very narrow eligibility criteria. For example, to meet the requirements for "durable medical equipment," a DHT would need to include specific types of hardware – which might exclude most software-only tools.

Another option when patients are remotely monitored by HCPs in between clinical visits, could be the use of billing codes that provide reimbursement for Remote Patient Monitoring (RPM), which covers evaluation and management of physiological data and Remote Therapeutic Monitoring (RTM), which covers review and monitoring of non-physiological data.[22] In these examples, the reimbursement is provided for the service that used the DHT, not for the technology itself – and the HCP would need to satisfy all of CMS's requirements for these billing codes.

One potential solution on the horizon, is the allocation of new funding for DHTs that meet the threshold for "breakthrough products" under the Ensuring Access to Breakthrough Products Act of 2024 (H.R. 1691).[23] This legislation will allow DHTs that qualify as breakthrough medical devices to receive four years of transitional reimbursement, with built-in requirements for CMS to create permanent reimbursement codes once FDA approval is granted.

CMS has similarly created a pilot for transitional coverage for breakthrough devices, under the Medicare Transitional Coverage for Emerging Technologies (TCET) program,[24] which was published in the Federal Register in August 2024. One helpful aspect of the TCET program is the creation of a process for submitting a non-binding letter of intent, alerting CMS 18-24 months in advance, that a DHT developer is seeking FDA approval for their product. This advance planning may allow more meaningful pre-launch planning and coordination between CMS, FDA, and DHT developers, to reduce regulatory and reimbursement uncertainty – which have proven to be key challenges for digital health.

History has shown that DHTs have not always been embraced until adoption is nurtured by regulatory reform or the availability of funding whether in the form of payor coverage, reimbursement, or incentive payments. In 2009, the American Recovery and Reinvestment Act provided of $27 billion in CMS funding payments for hospitals and clinics that adopted EHRs and could demonstrate satisfying certain criteria for "meaningful use" and attainment of related clinical quality measures.[25] This led to explosive growth in the deployment and use of EHR systems in the U.S., which according to one study, grew from 6.6% of U.S. hospitals in 2009 to 81.2% in 2019.[26] A similar effect was seen in the rapid growth of telemedicine during the COVID-19 pandemic, when CMS improved the ability to obtain reimbursement and waived a number of regulatory requirements that had effectively limited widespread adoption. To qualify for Medicare telehealth reimbursement, CMS temporarily: (i) waived requirements for pre-exiting established relationships with the billing HCP; (ii) waived certain patient and HCP location requirements for telemedicine; (iii) relaxed technology requirements for telehealth encounters, including permitting audio-only visits; and (iv) equalized reimbursement for telehealth visits to the same rate as in-person encounters.[27] One dataset showed that the number of telemedicine visits went from 0.1% of all billable encounters before the pandemic in 2019[28] to 4.86% in 2024.[29] While some of the CMS reforms that encouraged the growth of telehealth during the COVID pandemic will be sunset at the end of 2024, others have been made permanent.[30]

D. Regulation Under HIPAA

HHS-OCR is responsible for enforcing the Health Insurance Portability and Accountability Act (HIPAA).[31] Although HIPAA is commonly viewed synonymous with its most well-known section, the HIPAA Privacy Rule, which regulates the privacy of patients' health information, the original legislative intent of HIPAA, was broader and also included regulations focused on electronic health data access, interoperability, and portability. As health care and medical records become more digitized, these aspects of HIPAA have become more relevant. The Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted in 2009 to promote the safe use of health information technology and strengthened the privacy laws set forth by HIPAA.[32] The HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information and contains provisions that strengthen the civil and criminal enforcement of the HIPAA rules.

Digital health technology developers must ensure that DHTs subject to the HIPAA Privacy Rule and the HIPAA Security Rule are HIPAA-compliant to ensure that a patient's EHR or other health information is inaccessible to anyone other than the patient or their health care provider.

Non-HIPAA covered entities that develop and market DHTs should assess whether they might be subject state-level regulations or to federal regulation by the FTC or FDA. The FDA recently released draft guidance related to quality management and cybersecurity requirements for FDA-regulated medical devices that qualify as "cyber devices."[33] The draft guidance stressed that the criteria for cyber devices includes technology that is connected to the internet, including medical devices that incorporate: (i) wireless connectivity such as wi-fi or cellular technology, Bluetooth, radiofrequency communication; or (ii) hardwired connectivity capable of con-

necting to the internet, such as USB, ethernet, serial port and network, connections. Once deemed a "cyber device," the manufacturer of such devices would need to submit to FDA "a plan to monitor, identify, and address, as appropriate, in a reasonable time, postmarket cybersecurity vulnerabilities and exploits, including coordinated vulnerability disclosure and related procedures" in premarket device approval applications.[34]

III. Existing Clinical Uses of DHTs

Though the regulatory frameworks governing the development and use of DHTs continues to evolve, many DHTs have been successfully integrated into the health care sector. These technologies serve as helpful case studies to understand how DHTs can play an invaluable role in maximizing efficiency, expanding access to high-quality health care, and optimizing health outcomes.

A. Telehealth Platforms

Telehealth is the use of telecommunications and information technology to provide access to health assessments, diagnosis, intervention, consultation, supervision, and information across distance.[35] Using telehealth platforms, health care providers and patients are able to meet remotely, either over the phone or over a video call, to discuss a patient's symptoms, make a diagnosis, and identify a treatment plan. In conjunction with the patient's Electronic Medical Record (EMR) and the use of Artificial Intelligence (AI) – each discussed in more detail below – a physician can harness technology to accurately analyze the patient's symptoms, diagnose the patient, and prescribe medication.

This technology-supported process offers meaningful benefits for increasing access to health care, particularly for underserved populations, including those in rural areas or areas with limited access to care, and for patients suffering from infectious diseases, weakened immune systems, or otherwise compromised health. Additionally, telehealth increases provider efficiency, in large part by reducing the time that the provider spends with the patient and thereby allowing the provider to see more patients each day.

B. Remote Patient Monitoring Devices

Wearable health care technologies, or "wearables," are devices that patients can attach to themselves to allow their health care providers to remotely monitor their health. The most popular example of this is the Apple Watch. The Apple Watch is a consumer health product with an increasing range of built-in digital heath capabilities, including biometric hardware and software that monitors individuals' heart rate, sinus rhythm, blood oxygen, tracks the menstrual cycle, and can even detect a fall. While this is the most common example of a wearable, there are many other types of wearables that are used to track patients' health care trends, including, but not limited to, CPAP machines, blood pressure monitors, glucose meters, and heart monitors. A study by KLAS has shown that remote patient monitoring has successfully reduced hospital visits, reduced hospital readmissions, improved patient health, and overall, increased patient satisfaction.[36]

As with telehealth, wearables and other remote patient monitoring devices have had significant impact on facilitating access to care for patients who have historically been underserved. Wearables have also provided invaluable benefits by permitting patients to track and manage their own health and wellness, increasing knowledge and efficiency of whether and when care should be sought. Finally, these tools have proven invaluable in offering opportunities to improve medical outcomes and enhance efficiencies in the provision of health care by collecting significantly more real-world data on patients that can offer providers a more holistic view of patient health and inform care decisions.

C. Electronic Health Records

EHRs also allow for efficient transfers of patient data between patients and providers. Requesting and receiving a copy of a medical record can often be a tedious task for both patients and providers, and the use of EHRs allow patients to access their entire medical record at the click of a button. EHRs often allow all of the patient's providers to see their medical history, allowing for a smooth transfer of the medical record from one provider to another. EHRs can also be very useful if a patient suffers a medical emergency. At the push of a button, an EHR linked to an electronic health data sharing exchange such as the Statewide Health Information Network for New York (SHIN-NY) can quickly provide essential details to emergency responders in an emergency, such as preexisting medical conditions, prescriptions, allergies, and the contact information of the patient's primary care physician.

D. AI-Enabled Clinical Software

The use of AI can also increase the efficiency of HCPs by allowing for technology-enabled remote patient monitoring and machine learning to support diagnostic decision-making and analyze health trends. Real-world examples of AI-enabled software used in clinical settings may include, among other things, imaging systems that use algorithms to give diagnostic information for skin cancer in patients, and smart sensor devices that estimate the probability of a heart attack based on vital sign monitoring.[37] While the FDA has issued 950 approvals or authorizations for AI-enabled medical devices to date,[38] all of those approvals relate to algorithms that are "locked," meaning that such algorithms provide the same result each time the same input is applied and does not change with use.[39] While interest in the use of generative or adaptive AI continues to grow in the health care industry, the FDA and

other regulators are grappling with how to provide continue assurances of safety and effectiveness of such technologies.

IV. Ongoing Challenges with Uptake of DHTs

Despite the widespread use of these and other DHTs, it remains challenging for novel technologies to find an initial foothold in the health care space. Among the biggest barriers to rapid uptake of novel DHTs are entrenched patient and provider preferences; while younger and more technology-savvy patients may be enthusiastic about substituting traditional in-person medical care for the convenience of remote telemedicine visits, remote in-home diagnostics, remote chronic disease monitoring, and in-home treatment, many older patients prefer the traditional in-person experience and crave the face time (as opposed to FaceTime) with their medical providers.

A lack of digital literacy and access to digital tools may also remain barriers to the widespread adoption of DHTs. CDRH is currently working to address these factors to further assist low-income patients. In June of 2023, CDRH sought public comment on how to increase patient access to at-home use medical technologies. Advancing health equity was made part of CDRH's 2022-2025 strategic priorities.[40]

Even when DHTs are widely adopted, various challenges remain. For example, DHTs may create some ambiguity regarding responsibility for monitoring remotely acquired health data. There is some risk that patients may unreasonably expect HCPs to be actively monitoring data obtained by remote monitoring devices and alerting them to potential health risks. Until clinical care workflow models and medical standards of care evolve, many HCPs will be reluctant to assume responsibility for using advanced technology to actively monitor acute incidents in real time, for fear of liability over missed diagnoses.

Another significant risk associated with implementing DHTs to remotely care for patients is ensuring the accuracy of diagnoses and care decisions. Patients may be skeptical about whether HCPs can accurately provide a diagnosis without engaging in a physical, in-person assessment. Such apprehension may be born in large part from concerns about the shortcomings of existing telecommunications technology, the inability of HCPs to physically examine patients engaged in remote monitoring or telehealth visits, and social/communication barriers from not being in the same room.

Beyond patient skepticism, regulators like the FDA have reiterated their commitment to ensuring that DHTs that enter the marketplace are sufficiently accurate, reliable, and safe. The FDA's pre-market notification and pre-approval processes are invaluable stopgaps to provide assurances of the effectiveness and safety of FDA-authorized DHTs, but the FDA and other regulators have struggled to grapple with how to provide continued assurances of accuracy and reliability for novel, evolving DHTs including adaptive AI-enabled technologies that "learn" from real-world experience. Not only do such technologies raise concerns about validating constantly evolving algorithms to ensure ongoing reliability, but they also run the risk of incorporating bias into the provision of care based off of previous diagnoses or patterns of symptoms. AI bias can also cause health care discrimination, especially in marginalized communities. Studies have shown AI "compounding existing inequities in socioeconomic status, race, ethnicity, religion, gender, disability, or sexual orientation. Bias particularly impacts disadvantaged populations, which can be subject to algorithmic predictions that are less accurate or underestimate the need for care."[41] For these reasons, combating AI bias and establishing targeted regulatory frameworks to grapple with generative or adaptive AI have become key projects for regulators like the FDA.[42]

V. Conclusion

The emergence and rapid growth of digital health products presents myriad potential health benefits. The integration of telehealth, remote monitoring device, EHRs, and other existing DHTs has proven that these technologies offer opportunities to enhance efficiency in the health care sector, including by making scheduling and attending appointments with HCPs, as well as communicating historical health data between HCPs and patients, easier and more efficient. Additionally, DHTs have demonstrated their potential to expand access to high-quality, reliable care and to improve health outcomes by offering patients and HCPs a more holistic view of patient health. The potential for innovation in the field seems endless.

However, the development of DHTs and their integration into health care services also present various complex challenges. Concerns over data privacy and data security remain paramount, along with liability risks and health care compliance issues that may be faced. Hesitation to embrace DHTs remains a challenge among some patients, payors, and providers. Additionally, disparities in access to technology and digital literacy may exacerbate existing health care inequalities, posing ethical challenges that demand careful consideration. Government commitments to advancing health equity will bridge this gap by further providing enhanced access to health care, especially for those who reside in rural or low-income communities.

Despite these challenges, the transformative potential of digital health is undeniable. By fostering collaboration between health care providers, technology developers, policymakers, and patients, these obstacles can be overcome. With continued research and commitment to patient care, digital

health has the power to revolutionize the way we approach health care delivery, ultimately improving outcomes and enhancing the well-being of patients everywhere.

Emma N. Carey, J.D. 2024, Hofstra University School of Law, earned a Certificate of Excellence in Health Law for her academic achievements. Now an associate at Kerley, Walsh, Matera & Cinquemani, P.C., she focuses her practice on medical malpractice defense, dedicated to representing health care professionals and institutions.

Michael Purcell is a member of the life sciences regulatory and compliance practice group at Ropes & Gray in Washington, D.C. He focuses his practice on FDA regulatory matters and advises life sciences and health care clients on a broad range of regulatory and compliance issues under the Food, Drug and Cosmetics Act and related laws.

Jonathan Walland is Senior Corporate Counsel at Pfizer, where he provides strategic legal advice to help develop new drugs, vaccines, and digital health products for patients. Previously he was Associate General Counsel at the Memorial Sloan-Kettering Cancer Center in New York.

The authors would also like to thank Beth Roxland for her thought leadership and input on this article.

Endnotes

1. Food and Drug Administration, *What Is Digital Health?* https://www.fda.gov/medical-devices/digital-health-center-excellence/what-digital-health.
2. FDA, *Focus Area: Digital Health Technologies*, https://www.fda.gov/science-research/focus-areas-regulatory-science-report/focus-area-digital-health-technologies.
3. *See, e.g.,* FDA, *What Is Digital Health?*, https://www.fda.gov/medical-devices/digital-health-center-excellence/what-digital-health#benefits.
4. *See, e.g.,* FDA, *Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan* (Jan. 2021), https://www.fda.gov/media/145022/download; FDA, *Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD)* (Apr. 2019), https://www.fda.gov/media/122535/download.
5. *See, e.g.,* FDA, *Digital Health Software Precertification (Pre-Cert) Pilot Program*, https://www.fda.gov/medical-devices/digital-health-center-excellence/digital-health-software-precertification-pre-cert-pilot-program.
6. While state-level regulation – including health care professional licensure regulations, medical record-keeping laws, and emerging state privacy and anti-discrimination laws – does play a role in the regulation of DHTs, it will not be addressed in detail in this article.
7. 42 U.S. Code § 1320a–7b(b).
8. In 1976, the Medical Device Amendments Act was passed by Congress, which explicitly expanded FDA's authority to provide reasonable assurance of the safety and effectiveness of medical devices. *See* FDA, *A History of Medical Device Regulation & Oversight in the United States*, https://www.fda.gov/medical-devices/overview-device-regulation/history-medical-device-regulation-oversight-united-states; *see also* FDA, *Overview of Device Regulation*, https://www.fda.gov/medical-devices/device-advice-comprehensive-regulatory-assistance/overview-device-regulation.
9. 21 U.S.C. § 321(h)
10. 21 U.S.C. § 360j(o). Specifically, the 21st Century Cures Act excluded from the definition of "device" any "software function that is intended—

    (A) for administrative support of a health care facility, including the processing and maintenance of financial records, claims or billing information, appointment schedules, business analytics, information about patient populations, admissions, practice and inventory management, analysis of historical claims data to predict future utilization or cost-effectiveness, determination of health benefit eligibility, population health management, and laboratory workflow;

    (B) for maintaining or encouraging a healthy lifestyle and is unrelated to the diagnosis, cure, mitigation, prevention, or treatment of a disease or condition;

    (C) to serve as electronic patient records, including patient-provided information, to the extent that such records are intended to transfer, store, convert formats, or display the equivalent of a paper medical chart [subject to certain conditions] . . .;

    (D) for transferring, storing, converting formats, or displaying clinical laboratory test or other device data and results, findings by a health care professional with respect to such data and results, general information about such findings, and general background information about such laboratory test or other device, unless such

function is intended to interpret or analyze clinical laboratory test or other device data, results, and findings; or

(E) unless the function is intended to acquire, process, or analyze a medical image or a signal from an in vitro diagnostic device or a pattern or signal from a signal acquisition system, for the purpose of—(i) displaying, analyzing, or printing medical information about a patient or other medical information (such as peer-reviewed clinical studies and clinical practice guidelines); (ii) supporting or providing recommendations to a health care professional about prevention, diagnosis, or treatment of a disease or condition; and (iii) enabling such health care professional to independently review the basis for such recommendations that such software presents so that it is not the intent that such health care professional rely primarily on any of such recommendations to make a clinical diagnosis or treatment decision regarding an individual patient."

11. 86 Fed. Reg 41, 838 (Aug. 2, 2021).
12. *See, e.g.,* FDA, *Guidance for Industry: Policy for Device Software Functions and Mobile Medical Applications* (Sept. 2022), https://www.fda.gov/media/80958/download; FDA, *Guidance for Industry: Clinical Decision Support Software* (Sept. 2022), https://www.fda.gov/media/109618/download; FDA, *Guidance for Industry: Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices* (Sept. 2022), https://www.fda.gov/media/88572/download; FDA, *Guidance for Industry: General Wellness – Policy for Low Risk Devices* (Sept. 2019), https://www.fda.gov/media/90652/download.
13. FDA, *Guidance for Industry: Policy for Device Software Functions and Mobile Medical Applications*.
14. *See* FDA, *Digital Health Center of Excellence*, https://www.fda.gov/medical-devices/digital-health-center-excellence.
15. 21 CFR Part 800-822.
16. Jin J., *FDA Authorization of Medical Devices*. JAMA. 2014;311(4):435.
17. Van Norman, Gail A. *Drugs, Devices, and the FDA: Part 2: An Overview of Approval Processes: FDA Approval of Medical Devices*. JACC. Basic to Translational Science vol. 1,4; 277-287. 27 Jun. 2016, doi:10.1016/j.jacbts.2016.03.009.
18. *Id.*
19. Food and Drug Administration Safety A=and Innovation Act, 112 P.L. 144, 126 Stat. 993, 1054, 112 P.L. 144, 2012 Enacted S. 3187, 112 Enacted S. 3187, Section 607 Modification Of De Novo Application Process.
20. Federal Trade Commission, *What the FTC Does*, https://www.ftc.gov/news-events/media-resources/what-ftc-does.
21. DOH CMS Federal Register / Vol. 88, No. 70 / Wednesday, April 12, 2023 / Rules and Regulations.
22. Neha M. Matta and Catherine E. Robinson, *CMS Final Rules on Payment Impacts for Remote Therapeutic Monitoring*, June 26, 2023, https://frostbrowntodd.com/cms-final-rules-on-payment-impacts-remote-therapeutic-monitoring/, date accessed 7/30/2024.
23. Ensuring Access to Breakthrough Products Act of 2024 (H.R. 1691).
24. Centers for Medicare & Medicaid Services, Medicare Program; Transitional Coverage for Emerging Technologies, 89 Fed. Reg. 65724 (Aug. 12, 2024), https://www.federalregister.gov/documents/2024/08/12/2024-17603/medicare-program-transitional-coverage-for-emerging-technologies.
25. American Recovery and Reinvestment Act of 2009. Public Law. No. 111–5, Title XIII, Subtitle A-B.
26. John (Xuefeng) Jiang, Kangkang Qi, Ge Bai, Kevin Schulman, *Pre-Pandemic Assessment: A Decade of Progress in Electronic Health Record Adoption Among U.S. hospitals,* Health Affairs Scholar, vol. 1, issue 5, November 2023.
27. https://www.cms.gov/newsroom/fact-sheets/medicare-telemedicine-health-care-provider-fact-sheet, date accessed July 29, 2024.
28. Shaver J., *The State of Telehealth Before and After the COVID-19 Pandemic*. Prim Care. 2022 Dec;49(4):517-530.
29. Monthly Telehealth Regional Tracker | FAIR Health, date accessed July 29, 2024.
30. *Telehealth Policy Changes After the COVID-19 Public Health Emergency*, U.S. Department of Health and Human Services. https://telehealth.hhs.gov/providers/telehealth-policy/policy-changes-after-the-covid-19-public-health-emergency#temporary-medicare-changes-through-december-31,-2024.
31. Pub. L. 104–191.
32. Pub. L. 111–5.
33. FDA, *Draft Guidance for Industry: Select Updates for the Premarket Cybersecurity Guidance: Section 524B of the FD&C Act* (Mar. 2024), https://www.fda.gov/media/176944/download.
34. *Id.* at 4.
35. https://www.medicaid.gov/medicaid/benefits/telehealth/index.html.
36. Remote Patient Monitoring 2018; High Potential in a Shifting Landscape Remote Patient Monitoring 2018 | https://klasresearch.com/report/remote-patient-monitoring-2018-high-potential-in-a-shifting-landscape/1273KLAS Report (klasresearch.com).
37. *See* FDA, *Artificial Intelligence and Machine Learning in Software as a Medical Device*, https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device.
38. *See* FDA, *Artificial Intelligence and Machine Learning (AI/ML)-Enabled Medical Devices*, https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-aiml-enabled-medical-devices (last accessed Oct. 7, 2024).
39. *See* FDA, *Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD)*, fn.7 (Apr. 2019), *available at* https://www.fda.gov/media/122535/download.
40. *CDRH Seeks Public Comment on How to Increase Patient Access to At-Home Use Medical Technologies*, The FDA Law Blog. thefdalawbhttps://klasresearch.com/report/remote-patient-monitoring-2018-high-potential-in-a-shifting-landscape/1273log.com.
41. Mirja Mittermaier et al., *Bias in AI-Based Models for Medical Applications: Challenges and Mitigation Strategies*. Npj Digit. Med. 6, 113 (2023). https://www.nature.com/articles/s41746-023-00858-z.
42. *See, e.g.,* FDA, *Artificial Intelligence Program: Research on AI/ML-Based Medical Devices*, https://www.fda.gov/medical-devices/medical-device-regulatory-science-research-programs-conducted-osel/artificial-intelligence-program-research-aiml-based-medical-devices.

Washington State's My Health My Data Act: Implications for New York Entities

By Andria Adigwe and Sandra Fink

Washington State's My Health My Data Act (MHMDA or the "Act")[1] went into effect for all persons and entities, as defined in the Act, on June 30, 2024. As its name implies, the Act regulates how persons and entities collect, transfer and sell, or offer to sell, "consumer health data." The Act aims to close the gap between the current laws and consumers' expectations by protecting a consumer's health data that is not otherwise protected by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[2] This is consistent with Washington State's constitution, which guarantees a right to privacy.[3] The MHMDA is very broad in the definition of the data it protects and the persons and entities to which it applies.[4] MHMDA in essence aims to impose heightened consent requirements for collecting, processing, sharing, and selling consumer health data as well as impose procedures for consumers to be empowered to take charge of how their health data is being used. Washington State does not have a general data protection statute, but the MHMDA is the country's most extensive statute protecting consumer health data.

Persons and entities located in New York will need to be familiar and comply with this statute if their activities collect "consumer health data," as defined in the Act, of Washington citizens or those whose data was collected in the state.[5] This would occur, for example, if a person or entity (not necessarily in Washington State) operates a business, mobile application or website (or acts as a processor for such an entity) that is accessed by Washington residents, or people located in Washington, that may collect consumer health data in Washington.[6] And, of course, also if the entity wishes to transfer and/or sell, or offer to sell, the "consumer health data" that they collect.

This article will help persons and entities determine when the MHMDA may be applicable to their activities, summarize the corresponding requirements of the MHMDA, and provide practical considerations to promote compliance with the Act.

Scope of MHMDA

Definitions: Regulated Entities, Small Businesses, Persons and Processors

The Act is applicable to regulated entities, small businesses, persons and processors,[7] and reaches far beyond the limits of Washington State. A "regulated entity" is defined as: "any legal entity that: (a) conducts business in Washington, or produces or provides products or services that are targeted to consumers in Washington; and (b) alone or jointly with others, determines the purpose and means of collecting, processing, sharing, or selling of consumer health data." The Act goes on to clarify that government agencies or their contracted service providers, as well as tribal nations, are not included in the definition.

A small business is defined in the Act as a regulated entity satisfies one or both of the following thresholds: (a) collects, processes, sells, or shares consumer health data of fewer than 100,000 consumers during a calendar year; or (b) derives less than 50% of gross revenue from the collection, processing, selling, or sharing of the consumer health data, and controls, processes, sells, or shares consumer health data of fewer than 25,000 consumers. After June 30, 2024, a small business has the same requirement as a regulated entity. Small businesses only received extra time to implement MHMDA, until June 30, 2024, as opposed to March 31, 2024 for regulated entities.

There are particular sections where the Act uses the more expansive term "persons." A person includes those entities defined as regulated entities and small businesses, but also includes "natural persons." For instance, the term is used in sections pertaining to the processing of consumer health data, the sale of consumer health data and to restrictions on geofencing. These provisions are more broadly applicable to both regulated entities and also natural persons.

Which brings us to, last but not least, the processor of consumer health data, defined as "a person that processes consumer health data on behalf of a regulated entity or small business." "Processing" means "any operation or set of operations performed on consumer health data." Note that a person or entity that processes the data of a regulated entity may be subject to the law in their own right, and become a regulated entity, if they fail to adhere to their agreement with the regulated entity or small business to treat the consumer health data in accordance with the statute.[8] For example, all "affiliates, processors, contractors, and other third parties that receive notice of a consumer's deletion request shall honor the consumer's deletion request and delete the consumer health data from its records, subject to the same requirements of this chapter."[9]

Does the MHMDA Apply to You or Your Entity?

If an entity answers yes to any of the following questions, the MHMDA is likely to apply:

a. Does the entity conduct business (provide services or products) in Washington (whether to Washington residents or consumers passing through or located in Washington) through a website, mobile app, or otherwise, and collect, share, process or sell, or offer to sell, consumer health data (as defined below)?

b. Does the entity process data for a regulated entity?

c. Does an entity or person wish to implement a geofence around an entity that provides in- person health care services in the state of Washington?

Note that the Act is not limited by geography. New York-based entities, especially those with a web presence or a mobile application that is used by Washington State residents, or consumers located in Washington State, should pay close attention to MHMDA requirements. Except for those entities in industries regulated by agencies on the exemption list, no entity that collects consumer health data is beyond reach of the Act.[10] For instance, smart watches collecting blood/oxygen levels, or websites selling pregnancy tests to residents of, or travelers to, Washington State, need to carefully consider whether they comply with the Act.

Consumer Health Data Broadly Defined in the MHMDA

The Act aims to protect "consumer health data" which it defines as "personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status." The Act goes on to provide a non-exhaustive list of information that is within the definition:

- Individual health conditions, treatment, diseases, or diagnosis;
- Social, psychological, behavioral, and medical interventions;
- Health-related surgeries or procedures;
- Use or purchase of prescribed medication;
- Bodily functions, vital signs, symptoms, or measurements of the information described in this (list of data types covered by the Act);
- Diagnoses or diagnostic testing, treatment, or medication;
- Gender-affirming care information;
- Reproductive or sexual health information;
- Biometric data;
- Genetic data;
- Precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies;
- Data that identifies a consumer seeking health care services; or
- Any information that a regulated entity or a small business, or their respective processor, processes to associate or identify a consumer with the data described above that is derived or extrapolated from non-health related information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning).[11]

Although the Act seemingly touches on a wide variety of health care data, it also sets limits as to its applicability. The Act explicitly exempts information already protected by HIPAA (healthcare information), Gramm-Leach-Bliley Act (financial information), Family Education Rights and Privacy Act (educational information), Fair Credit Report Act (credit information), or data utilized in research that is subject to review by an institutional review board or similar body.[12] This list of exemptions illustrates how expansive the Act actually is; if data does not fall into these specifically regulated buckets, it is potentially covered.

A comparison with HIPAA's definition of Protected Health Information (PHI) and the Federal Trade Commission's (FTC) definition of personal health record (PHR) "identifiable health information," as discussed herein, demonstrates how much broader the MHMDA definition is.

The Broader Context: Abortion and Gender-Affirming Care

MHMDA is a sign of the times, and its passage reflects the political and social context. Representative Vandana Slater described the need for the Act as follows: "In the aftermath of regressive policies passed by neighboring states and a major reversal of the *Roe* decision by the U.S. Supreme Court, this bill is an urgent and critical step to protect the privacy of personal health care decisions."[13] It is therefore unsurprising that certain politically debated topics are explicitly mentioned, such as reproductive care, gender-affirming care, and precise location reasonably connected to a consumer's attempt to obtain medical care. Other federal and state privacy laws, drafted during different times and different contexts, have not specifically listed topics that are on voting ballots.

Recently Litigated Limitations of HIPAA: Website Tracking Technologies

HIPAA is the federal law that addresses the protection of health data through its privacy rule. If applicable, HIPAA's privacy rule requires, among other things, prior written patient consent for the collection or sharing of PHI (including when sharing with vendors, which requires a separate business associate agreement), notification to patients of their privacy rights and how their information will be used, and the granting of patient access to their PHI. However, unlike MHMDA, which does not distinguish between medical pro-

viders and other types of entities in its definition of regulated entities, HIPAA's application is limited to health care providers, health care insurance companies and health care clearinghouses ("covered entities"). The definition of individually identifiable, and therefore protected, health information under HIPAA is considerably more limited than MHMDA.

Like the Washington legislature, HHS, which administers HIPAA, grew concerned that website tracking technologies could expose health information of patients as they visited the websites of the covered entities. To address this concern, HHS issued a guidance document in December of 2022,[14] in which HHS provided several hypotheticals that would trigger HIPAA obligations, "including circumstances where an online technology connects (1) an individual's IP address with (2) a visit to a UPW (unauthenticated public web page) addressing specific health conditions or healthcare providers."[15] This very protection was vacated by a Texas Federal District Court, which recently held that HIPAA's privacy rule could not apply to website tracking technologies on covered entities' unauthenticated (not password protected) websites. The court reasoned that such information could not, as a matter of law, fall within HIPAA's statutory definition of individually identifiable health information (IIHI), which, the court explained, is "unambiguously defined as PHI, that (1) 'relates to' an individual's 'past, present, or future physical or mental health or condition,' the individual's receipt of 'health care,' or the individual's 'payment for' healthcare; *and* (2) 'identifies the individual' or provides 'a reasonable basis to believe that the information can be used to identify the individual.'"[16]

The Court distinguished between a covered entity's authenticated website (where an individual will need to log into an account) and unauthenticated websites (where no log-in password is required). The Court agreed with the plaintiffs and vacated the portion of the bulletin to the extent that HIPAA would be triggered solely by the connection between an individual's IP address and "a visit to a[n] [unauthenticated public webpage] addressing specific health conditions or healthcare providers." The Court held that "without *knowing* a particular query relates to a category of information in Section 1320d(6), metadata from a[n unauthenticated website] search cannot constitute [PHI]. To hold otherwise would empower HHS and other executive entities to take increasingly expansive liberties with the finite authority granted to them." HHS therefore placed a note in its bulletin that "HHS is evaluating its next steps in light of that order."

HHS' position, as explained in its bulletin, was that HIPAA may not apply when information collected on unauthenticated website did not relate to an individual's PHI (e.g. ,a search of a hospital's job postings or visiting hours, or a student browsing the unauthenticated website of a cancer hospital for a paper.) However, if that same individual is browsing that same unauthenticated website to find a doctor for a second opinion, that information would be considered PHI, according to the guidance; the question was one of fact and the covered entity was held to have shared PHI if the facts so demonstrated. This meant that covered entities had to treat all searches whether on authenticated or non-authenticated websites as PHI.

Under MHMDA, however, this very data, from a covered entity's unauthenticated, public-facing website, may be considered consumer health data, depending on inferences that may be drawn by the covered entity (or any other regulated entity under the Act.) particularly as the MHMDA includes "personal information" within "consumer health data" as: "information that identifies or is reasonably capable of being associated or linked, directly or indirectly, with a particular consumer," and specifically includes, but is not limited to "data associated with a persistent unique identifier, such as a cookie ID, an IP address, a device identifier, or any other form of persistent unique identifier."[17]

In its "Frequently Asked Questions," the Washington State attorney general answered a question about organizations drawing inferences from purchases that could be considered consumer health data.[xxvi] The question and answer are as follows:

> If a regulated entity or small business draws inferences about a consumer's health status from purchases of products, could that information be considered consumer health data?
>
> Yes. The definition of consumer health data includes information that is derived or *extrapolated from nonhealth data when that information is used by a regulated entity or their respective processor to associate or identify a consumer with consumer health data.* This would include potential inferences drawn from purchases of toiletries. For example, in 2012 the media reported that a retailer was assigning shoppers a "pregnancy prediction score" based on the purchase of certain products; this information is protected consumer health data even though it was inferred from nonhealth data. *Likewise, any inferences drawn from purchases could be consumer health data.*
>
> In contrast, nonhealth data that a regulated entity collects but does not process to identify or associate a consumer with a physical or mental health status is not consumer health data.[18]

Applying that answer in practice, if inferences could be drawn from data stemming from online purchases, considering the use of tracking technology to collect IP addresses or device IDs, it is very likely that the information will be associated with an individual – thus becoming a consumer health data if within the Act's definition. MHMDA does not seemingly hinge on the visitor's motivation, which was frowned upon by the Texas Court, but hinges on the actions of persons or regulated entities (drawing inferences). In the meantime, there is no bright line rule and the application of HIPAA to websites and apps, similar to the application of MHMDA, can be extremely context, and fact, specific.

And, keep in mind that MHMDA applies to regulated entities, which include but go beyond health care entities, albeit with some Washington State connection. As the politics around sensitive health care topics continues to shift and the proliferation of internet and app use in the health arena develops, it is likely that additional, potentially more expansive, legislation will be passed in the future, whether on the state or federal level.

Context: Other Applicable Laws and Guidance Besides the Act and HIPAA

New York Attorney General Guidance and New York's Consumer Protection Laws

New York State lacks its own comprehensive consumer data privacy law but the New York attorney general recently issued guidance on website privacy controls focused on tracking technologies for New York businesses[19] (and consumers),[20] which confirms that businesses' privacy-related practices and statements are subject to New York's consumer protection laws,[21] and explains that these laws require that websites' representations concerning consumer privacy "be truthful and not misleading. This means that statements about when and how website visitors are tracked should be accurate, and privacy controls should work as described." Recent cases have confirmed that New York consumer protection laws apply in the context of consumer privacy.[22]

Entities maintaining websites that market to New York consumers must clearly and properly characterize all tracking technologies deployed, deploy consent management tools that respond to a consumer's answers and avoid any deceptive practices. As an example, the AG called out websites that deploy cookies as soon as a visitor reaches the website, but somehow give the impression that the visitor can decide whether or not cookies are deployed (e.g., by using a cookie pop-up that states that a user has to "accept" cookies).

The FTC

Regarding health data of consumers, New York entities must also comply with the Federal Trade Commission's Health Breach Notification rule (HBNR),[23] which requires vendors of personal health records, and related entities, to notify consumers following a breach involving unsecured information. The FTC, recognizing the speed in which technology is progressing, decided to step into an apparent gap left by HIPAA by updating the HBNR in May of 2024, effective July 20, 2024.[24] Samuel Levine, director of the FTC's Bureau of Consumer Protection, stated, "With the increasing use of health apps and connected devices, the updated HBNR will ensure it keeps pace with changes in the health marketplace." FTC now requires entities "that are not covered by [HIPAA] to notify individuals, the FTC, and, in some cases, the media of a breach of unsecured personally identifiable health data."[25] Similar to HIPAA, PHR identifiable health information means information that:

> (1) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and
>
> (i) Identifies the individual; or
>
> (ii) With respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

Practical Considerations for Compliance With MHMDA

Most New York entities that operate a website or app are providing notice of their privacy policies and enabling consumer to opt out of consent for sharing of their data. The MHMDA requires New York entities to implement additional privacy controls as related to consumer health data if the entity engages in the activities as described above, and is a regulated entity under the MHMDA.

What Is Required for Compliance With the MHMDA

MHMDA has requirements for: (a) the collection of consumer health data; (b) the sharing of consumer health data; and (c) the sale, or offer to sell, consumer health data. All require prior opt-in consent and an applicable privacy policy but the requirements applicable to each of these actions are different and must be understood separately. In addition, MHMDA establishes geofencing rules that will need to be complied with. Washington State residents are provided with rights to control what kind of data is collected, how it is collected, and how, if at all, it is shared or sold. And the Act provides the right to request deletion of data and requires an appeal procedure to be provided to consumers.[26]

Separate Privacy Policy with a Separate Link on Home Page

A regulated entity must maintain a consumer health data privacy policy that clearly and conspicuously discloses specific information as described below. This consumer health data privacy policy must be "a separate and distinct link on the regulated entity's homepage and may not contain additional information not required under the My Health My Data Act."[27]

The consumer health data privacy policy must include:

1. The categories of consumer health data collected and the purpose for which the data is collected, including how the data will be used;

2. The categories of sources from which the consumer health data is collected;

3. The categories of consumer health data that is shared;

4. A list of the categories of third parties and specific affiliates with whom the regulated entity or the small business shares the consumer health data; and

5. How a consumer can exercise the rights provided in the MHMDA to withdraw consent from the regulated entity's collection and sharing of consumer health data concerning the consumer and request deletion of such data, in WA ST 19.373.040.

Separate Opt-in Consent for Collecting and Sharing

Regulated entities must obtain opt-in consent for the collection or sharing of consumer health data, unless the collection or sharing of the data is "necessary to provide a product or service that the consumer has requested from the regulated entity or small business." The consent to share consumer health data must be "separate and distinct from the consent obtained to collect the data."[28]

The consent for collecting and/or sharing consumer health information must clearly and conspicuously disclose the following:

1. The categories of consumer health data collected or shared;

2. The purpose of the collection of sharing of the consumer health data, including the specific ways in which it will be used;

3. The categories of entities with whom the consumer health data is shared; and

4. How the consumer can withdraw consent from future collection or sharing of the consumer's health data.[29]

Sale or Offer of Sale of Consumer Health Data

The requirements discussed in this section have been called so onerous that "it is unlikely many companies will even attempt to seek an authorization to sell, resulting in a de facto prohibition on most activities that could constitute a 'sale' including much third-party targeted advertising."[30]

Here is what is required in the separately signed, one-year maximum, specific authorization for the sale, or offer of sale, of consumer health data:

a. The specific consumer health data concerning the consumer that the person intends to sell;

b. The name and contact information of the person collecting and selling the consumer health data;

c. The name and contact information of the person purchasing the consumer health data from the seller;

d. A description of the purpose for the sale, including how the consumer health data will be gathered and how it will be used by the purchaser when sold;

e. A statement that the provision of goods or services may not be conditioned on the consumer signing the valid authorization;

f. A statement that the consumer has a right to revoke the valid authorization at any time and a description on how to submit a revocation of the valid authorization;

g. A statement that the consumer health data sold pursuant to the valid authorization may be subject to redisclosure by the purchaser and may no longer be protected by this section;

h. An expiration date for the valid authorization that expires one year from when the consumer signs the valid authorization; and

i. The signature of the consumer and date.[31]

Geofencing

Geofencing involves setting up a virtual perimeter around a specific geographic zone or location. Geofencing can be used to deliver location-based advertisements, for instance. Entities could do this by themselves or through a vendor.

Similar to the law of New York,[32] and using a similar definition of "geofencing," the MHMDA prohibits implementing a geofence around an entity that provides in-person health care services where such geofence will identify or track consumers seeing health care services, collect consumer health data from such consumers or send notifications, messages or advertisements to consumers related to their consumer health data or health care services.[33]

Consumer Rights Will Require Entity Policies and Procedures

Similar to the European Union's General Data Protection Regulation, and other state comprehensive consumer data

protection laws, the MHMDA will require regulated entities to adopt policies and procedures to implement the rights granted by the statute. For example, those whose data was collected under the Act have rights to:

a. Confirm whether a regulated entity or small business is collecting, sharing, or selling consumer health data concerning the consumer;

b. Access such data;

c. Access a list of all third parties and affiliates with whom the regulated entity or small business has shared or sold the consumer health data; and

d. Obtain an active email address or other online mechanism that the consumer may use to contact the third parties with whom the regulate entity or small business has shared or sold the consumer health data;

e. Withdraw consent from the regulated entity's or the small businesses' collection and sharing of consumer health data concerning the data;

f. To have the consumer health data concerning the consumer deleted and to exercise that right by informing the regulated entity or the small business of the consumer's request for deletion;

g. To have the request for deletion of data communicated to the affiliates, processors, contractors and other third parties with whom the regulated entity or the small business has shared the consumer health data.

Regulated entities and small businesses must procedurally address requests that stem from these rights under the Act. Regulated entities must make a secure and reliable means for the consumer to exercise their rights, which shall be described in the consumer health data privacy policy.

Note that the regulated entity has 45 days to reply to consumer requests.[34] Also, similar to Texas law, consumers under the MHMDA have the right to appeal a failure to act or an adverse decision made by the regulated entity. Organizations therefore need to create a mechanism to meet this requirement for an appeal process and, if the appeal is denied, the entity "shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the attorney general to submit a complaint."[35] Which leads to the topic of enforcement.

Enforcement

The MHMDA's is enforced by the attorney general and by individual consumers exercising their private right of action. Enforcement specifically incorporates enforcement provisions of Washington state's Consumer Protection Act (CPA), stating that a violation of the Act is a per se violation of the CPA, and constitutes "an unfair or deceptive act in trade or commerce and an unfair method of competition for the purpose of applying the consumer protection act, chapter 19.86 RCW."[36] The Washington Consumer Protection Act does not include statutory damages and plaintiffs will have to show causation and injury to the plaintiff's "business or property" to recover actual damages.

Conclusion: Impact on New York Companies and Enforcement Concerns

More and more states are placing greater emphasis on protecting health care and biometric information.[37] By any measure, MHMDA is far reaching, cross-industry Act that provide Washington residents (and tourists) a level of autonomy over their health care data that dwarfs other statutes. New York entities, both healthcare and non-healthcare, with an online presence, or an app that reaches Washington State, will need to take that statute into account as they stay abreast of the patchwork of data privacy laws that are increasingly appliable. In addition to the policies and procedures to effectuate consumer rights related to data, entities will need to employ appropriate privacy and cyber security hygiene on their websites and apps, such as creating hyperlinks, pop-up notices and opt-in consent buttons that are clear and equal in size, color, and emphasis. At all cost, entities should avoid misleading language, interfaces or practices on their websites and apps and should be encouraged to consult an attorney in this field to stay compliant with all applicable laws and regulations. If any statute can make the case for this, it is the MHMDA.

Andria Adigwe is a regulatory health law and data privacy and cybersecurity attorney at Buchanan Ingersoll Rooney, PC, and co-chair of the E-Health Committee of NYSBA's Health Law Section. She assists clients through complex mergers and acquisitions, provides regulatory guidance on operational questions, and advises them on data privacy and cyber security compliance issues.

Sandra Fink is a licensed attorney in New York and Maryland, with IAPP CIPP/US certification. She is also a student in the advanced certificate track in cybersecurity and data privacy at Albany Law School and is a member of the New York City Bar Association's Technology, Cyber and Privacy Law Committee.

Endnotes

1. Chapter 19.373. Washington My Health My Data (MHMD) Act. (WA ST 19.373.005 TO 19.373.900).
2. WA ST 19.373.005. According to Washington State's attorney general, "The My Health My Data Act is the first privacy-focused law in the country to protect personal health data that falls outside the ambit of . . . HIPAA," https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy. The statute also specifically states, "HIPAA only covers health data covered by specific health care entities, including most health care providers. Health data collected by noncovered entities, including certain apps and websites, are not afforded the same protections. Chapter 191, Laws of 2023 works to close the gap between consumer knowledge and industry practice by providing stronger privacy protections for all Washington consumers' health data." WA ST 19.373.005.
3. Washington State Constitution Article 1, § 7 provides: "INVASION OF PRIVATE AFFAIRS OR HOME PROHIBITED. No person shall be disturbed in his private affairs, or his home invaded, without authority of law."
4. "Further, the Act is extremely broad in terms of the types of data covered and the entities that are subject to it. As a result, many companies (and nonprofits) that don't think of themselves as handling health data are surprised when they learn that they may be subject to the Act's obligations." Mike Hintz, *The Washington My Health My Data Act: Not Just Washington (Or Health)*, California Lawyers Association, Privacy Law Section Journal, Volume 1, 2024, https://calawyers.org/privacy-law/the-washington-my-health-my-data-act-not-just-washington-or-health.
5. *Id.*
6. "Consumer" includes both Washington residents and individuals whose consumer health data is collected in Washington, which could be an individual who resides elsewhere and is temporarily in Washington where their information is obtained. WA ST 19.373.010(7).
7. Definitions are found in WA ST 19.373.010.
8. WA ST 19.373.060 (1)(c).
9. WA ST 19.373.040(1)(C)(ii).
10. Those obligations are extensive, in several cases going well beyond what we have seen with any other privacy law. The sweeping scope and extreme substantive obligations, combined with vague terms and a private right of action, make this Act extraordinarily challenging and risky for a very wide range of organizations." Hintze, *supra* note 4.
11. WA ST 19.373.010 (8)(b)(i) - 8(b)(xiii). *See also,* Washington State Office of the Attorney General Frequently Asked Questions (FAQ), Question #6, https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy.
12. WA ST 19.373.010 (8)(c) and RCW 19.373.100. Exemptions.
13. Vandana Slatter, *Governor Inslee Signs WA My Health, My Data Act Into Law,* April 27, 2023, https://housedemocrats.wa.gov/slatter/2023/04/27/governor-inslee-signs-wa-my-health-my-data-act-into-law/.
14. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html. *See also* Health and Human Services, *HHS Office for Civil Rights Issues Bulletin on Requirements Under HIPAA for Online Tracking Technologies To Protect the Privacy and Security of Health Information*, December 1, 2022, https://www.hhs.gov/about/news/2022/12/01/hhs-office-for-civil-rights-issues-bulletin-on-requirements-under-hipaa-for-online-tracking-technologies.html. After the Bulletin was challenged, the HHS amended it in spring of 2024, but not as concerns the intent to protect consumers information on non-authenticated websites. Health and Human Services, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates,* March 18, 2024, Rev. June 26, 2024, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html .
15. *Id.*
16. *American Hospital Association et al. v. Berreca et al,* ___F. Supp. 3d ___, 2024 WL 3075865 (June 20, 2024), citing 42 U.S.C. § 1320d(6).
17. WA ST 19.373.010(18)(a).
18. https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy. Question 6.
19. New York Attorney General, Website Privacy Controls: A guide for Business, https://ag.ny.gov/resources/organizations/business-guidance/website-privacy-controls (Rev. July 15, 2024).
20. New York Attorney General, *A Consumer Guide to Web Tracking,* https://ag.ny.gov/publications/consumer-guide-web-tracking (Rev. July 15, 2024).
21. NY Gen Bus Ch. 20, Art. 22-a.
22. *See, e.g., Elliot Libman, et al. v. Apple, Inc.*, 2024 WL 4314791 (N.D. Cal, slip op. September 26, 2024) (finding plaintiff stated a claim under New York Gen. Bus. Law § § 349 and 350 and survived a Motion to Dismiss under Rule 12(b)(6) where plaintiff alleged "purported misrepresentations made via Apple's "share [Device] Analytics" setting."
23. 16 CFR Part 318.
24. 89 FR 46028, available at https://www.federalregister.gov/documents/2024/05/30/2024-10855/health-breach-notification-rule.
25. Federal Trade Commission, *FTC Finalizes Changes to the Health Breach Notification Rule,* April 26, 2024, available at https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-finalizes-changes-health-breach-notification-rule.
26. WA ST 19.373.040.
27. WA ST 19.373.020.
28. WA ST 19.373.030(1)(b)(i).
29. WA ST 19.373.030(1)(c).
30. Hintze, *supra* note 4.
31. WA ST 19.373.070.
32. N.Y. Gen Bus § 394-g, "Geofencing of health care facilities."
33. WA ST 10.373.080.
34. WA ST 19.373.040 (1)(g).
35. WA ST 19.373.040 (1)(h).
36. *See also,* Washington State Office of the Attorney General FAQ, Question 2, https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy. The FAQ states: "Section 11 of the My Health My Data Act provides that any violation of the Act is a per se violation of the Washington Consumer Protection Act (CPA), WA ST 19.86, which is enforced by the Attorney General as well as through private action." (#2) https://www.atg.wa.gov/protecting- washingtonians-personal-health-data-and-privacy.
37. For example, Nevada's SB 370 requires the protection of consumer health data but defines consumer health data more narrowly and lacks a private right of action for consumer.

Federal Interoperability Initiatives and Opportunities for New York State Participation

By Puja Khare and Mekleet Teferi

I. Introduction

For more than a decade, the U.S. Department of Health and Human Services (HHS) has aimed to increase health care provider adoption of universal Certified Electronic Health Record Technology (CEHRT) to improve access to electronic health information by patients and their treating providers.[1] In recent years, HHS has advanced initiatives that include additional sharing, including between competitor electronic health record (EHR) vendors, health information networks, health insurers, public health agencies, and care management organizations.[2]

The legal underpinning for this expansion is the 21st Century Cures Act, which became law in 2016.[3] Congress recognized that information sharing was disparate and directed HHS's Office of the National Coordinator for Health IT (ONC) to, among other things, convene stakeholders to develop a trusted exchange framework and a common agreement for nationwide exchange between health information networks. In 2018, ONC released the first set of supporting materials for this initiative, known as the Trusted Exchange Framework and Common Agreement (TEFCA).[4] TEFCA is intended to advance the nationwide sharing of electronic health information to foster better clinical decision-making, improve clinical and quality outcomes, and lower costs.[5] It is the leading policy driver of the push to increase interoperability at the federal level, with implications for state-level health information exchange.

It bears noting that national health information-sharing networks existed prior to TEFCA.[6] Many health care organizations participate in these networks today to support clinical decision-making and improve quality and patient outcomes. One of these national networks is Carequality.[7] The EHR vendor Epic was a founding member of and currently participates in the Carequality network.[8] For context, Epic covers more than half of U.S. acute care hospital beds, holding approximately 39.1% of hospital market share.[9] Today, all of Epic's U.S.-based hospital and clinic customers participate in Carequality.[10] Similarly, many providers and government entities are connected to another large national network, eHealth Exchange. eHealth Exchange participants include

the U.S. Food and Drug Administration, U.S. Department of Veteran Affairs, and several state health information exchange organizations.[11]

However, these networks operate independently with unique legal agreements, which has resulted in siloed data.[12] Thus, some organizations must join multiple networks to achieve meaningful exchange. Also, non-care delivery entities such as health insurers and public health agencies have not traditionally participated to the same extent as providers. TEFCA therefore has three goals: 1) establish a universal governance, policy, and technical floor for nationwide interoperability; 2) simplify connectivity for organizations to securely exchange information to improve patient care, enhance the welfare of populations, and general health care value; and 3) enable individuals to gather their health care information.[13]

II. The Basics of TEFCA

ONC defines the overall policy and governance requirements for TEFCA.[14] ONC has designated the Sequioa Project, an independent not-for-profit entity, as the Recognized Coordinating Entity (RCE) tasked with implementing TEFCA.[15] ONC also designates Qualified Health Information Networks (QHINs) to facilitate the exchange of information.[16] QHINs are generally health information exchange organizations with a proven history of exchanging health care information among participants.[17] The RCE provides the oversight and governing approach for QHINs. QHINs connect directly with each other to share information for specific purposes.

Hospitals, health insurers, public health agencies, and others connect to QHINs as participants and make requests of each other for information.[18] QHINs facilitate the requests and responses. Each QHIN must sign the same Common Agreement (CA) with the RCE, which defines the legal and technical requirements for secure information sharing.[19] For participants and sub-participants connecting to TEFCA before July 1, 2024, the CA also contains certain provisions that the QHIN must flow down to their participants, including how participants may use or disclose TEFCA information.[20] Any new participants or sub-participants will sign a Terms of Participation.[21] TEFCA also considers connections by patients, but as sub-participants, such as through a patient portal app offered by a hospital or other consumer health app. The RCE hosts a directory that allows for identification of QHINs, participants, and sub-participants, to send messages and query for data.

There are currently six exchange purposes authorized under the CA: treatment, payment, health care operations, public health, government benefits determination and individual access services.[22] Exchange is governed by the requirements in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as well as any other applicable law, such as state law. There are also comprehensive standard operating procedures (SOPs) and technical requirements for each exchange purpose, both of which are developed by private and public stakeholders.

The treatment exchange purpose SOP was released in 2024. Of relevance here, the RCE is in the process of establishing the SOP and technical requirements for public health exchange. The most recent draft allows participants to exchange for public health, as defined by HIPAA, electronic case reporting, and electronic laboratory reporting.[23] The U.S. Centers for Disease Control and Prevention is currently piloting this exchange with several state and local public health agencies (PHAs).[24] The RCE notes that it "anticipates judiciously expanding" the public health exchange purposes over time to address additional priorities, including prescription drug monitoring, hospital capacity, and chronic disease.

Importantly, TEFCA exchange is intended to be bi-directional, which means participants across the spectrum – providers, health insurers, public health agencies, etc. – can request data from and share data with each other. Although TEFCA participation is currently voluntary for entities, the federal government incentivizes participation by offering TEFCA participation as a means of meeting certain regulatory requirements.[25]

The first set of QHINs were designated in early 2023, based on an application and vetting process. There are currently seven designated QHINs, including one affiliated with Epic and another with eHealthExchange.[26] Although there are no public statistics on how much data is being exchanged via TEFCA, QHINs continue to publish growing lists of entities that have committed to participate in their networks.[27] Notably, Epic recently announced that it plans to fully move its interoperability activity from Carequality to TEFCA by the end of 2025.[28]

III. Opportunities for New York State Involvement in TEFCA

The forward movement on interoperability at the federal level raises the question of how and to what extent states should be involved. Similar to TEFCA's goals, New York State is committed to the concept of streamlining. Governor Kathy Hochul proposed – and the Legislature approved – a $2.5 million allocation in New York's fiscal year 2024 budget to modernize health care reporting systems in an effort to, in part, alleviate provider reporting burden.[29]

State health departments such as the New York State Department of Health (DOH) wear many hats, including PHA and Medicaid payer, both of which are TEFCA participants. As previously mentioned, several other states, via their

health information exchange networks, are currently part of the eHealth Exchange national network, which may serve as their onramp to TEFCA. New York State's health information network, the Statewide Health Information Network (SHIN-NY), has existed for almost two decades.[30] In fact, the SHIN-NY operated under a TEFCA-like structure well before TEFCA was even contemplated. In this regard, the state designated the New York eHealth Collaborative (NYeC) to lead and coordinate the SHIN-NY, working closely with DOH. Hospitals, clinics, federally qualified health centers, and others are required to connect to a regional health information network, called a Qualified Entity (QE), and upload certain patient information.[31] Patients must opt-in to share their information with the SHIN-NY. There are currently six different QEs. The QEs allow participating entities to access electronic health information with patient consent.

This year, DOH finalized comprehensive changes to the SHIN-NY regulations.[32] The amendments introduce the concept of a data repository, where QEs would be required to send specific data from its participants, such as hospitals. The state would then have access to data in the repository for public health and Medicaid purposes. These amendments are a significant operational shift from the current SHIN-NY structure in which DOH must make a request of each QE individually to receive participant data. It is expected that comprehensive data governance and technical requirements will be established to govern this activity, including determining what data should be sent to the repository.

The impetus for these changes is to support the state's activity under the New York Medicaid Redesign Team section 1115 demonstration, known as the "1115 waiver."[33] The 1115 waiver is set to bring approximately $8 billion into the state, $4 billion of which is dedicated to addressing health equity by screening patients for social needs and making appropriate referrals. The SHIN-NY will be the information-sharing vehicle for this initiative. The state also has an interest in using the data repository structure to improve their response to public health emergencies.

Some of DOH's recent goals are aligned with the benefits to state governments and PHAs to participate in TEFCA, including improving access to population health data, further advancing interoperability for Medicaid, and facilitating bi-directional exchange with PHAs. And, as a payer, DOH could have easier access to the necessary data for case management, quality measurement and reporting activity, and risk adjustment activity under TEFCA. Thus, there is an opportunity for the state to further explore TEFCA participation.

IV. Conclusion

ONC's TEFCA initiative will continue to evolve and expand in the years to come. Given the RCE's commitment to "judicially expand" the public health exchange purpose, TEFCA exchange may eventually fully align with DOH's goals. Moreover, New York State's participation in TEFCA could allow for the streamlining of public health data collection and alleviate provider reporting burdens. Although there are still issues to be addressed, including alignment of consent structures, it could be valuable for New York State to consider how joining TEFCA may augment their efforts.

Puja Khare is Vice President of Legal, Regulatory, and Professional Affairs at the Greater New York Hospital Association. She provides member support on legal and regulatory issues, including health information privacy and security, digital health, and medical-legal matters. She can be reached at pkhare@gnyha.org.

Mekleet Teferi is Assistant Director of Regulatory Affairs at the Greater New York Hospital Association. She is responsible for a broad range of operational and regulatory subject areas, including privacy and health information technology issues, artificial intelligence, and research compliance. She can be reached at mteferi@gnyha.org.

Endnotes

1. *See generally* The American Recovery and Reinvestment Act of 2009. H.R. 1, 111th Cong. (2009). https://www.govinfo.gov/content/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf.
2. *See e.g.*, 2020-2025 Federal Health IT Strategic Plan, https://www.healthit.gov/topic/2020-2025-federal-health-it-strategic-plan; Information Blocking, 45 CFR Part 171 (2020).
3. *See* 21st Century Cures Act, Pub. L. No. 114-255 (2016).
4. *See* Genevieve Morris, *Trusted Exchange Framework and Common Agreement: A Common Sense Approach to Achieving Health Information Interoperability*, HealthITBuzz (January 5, 2018), https://www.healthit.gov/buzz-blog/interoperability/trusted-exchange-framework-common-agreement-common-sense-approach-achieving-health-information-interoperability.
5. *See What Is the Trusted Exchange Framework and Common Agreement™*?, https://rce.sequoiaproject.org/tefca/.
6. *See generally* HIMSS, *Understanding National Interoperability Frameworks and Networks*, https://www.himss.org/sites/hde/files/media/file/2024/08/02/himss_interopframeworks_ebook-2.pdf.
7. *See supra* n. 6; *see also* Carequality, https://carequality.org/.

8. *See* Carequality, *athenahealth, eClinicalWorks, Epic, NextGen Healthcare and Surescripts First to Adopt Carequality Interoperability Framework*, Carequality Blog (January 21, 2016), https://carequality.org/athenahealth-eclinicalworks-epic-nextgen-healthcare-and-surescripts-first-to-adopt-carequality-interoperability-framework/.

9. *See* Giles Bruce, *Epic's Dominance in 12 Numbers,* Becker's Health IT (July 18, 2024), https://www.beckershospitalreview.com/ehrs/epics-dominance-in-12-numbers.html (citing Tyson Blauer & Paul Warburton, *US Acute Care EHR Market Share 2024*, KLAS Research (May 17, 2024), https://klasresearch.com/report/us-acute-care-ehr-market-share-2024-large-organizations-drive-market-energy/3333).

10. *See Leading Health Systems Pledge To Join TEFCA* (May 22, 2023), https://www.epic.com/epic/post/leading-health-systems-pledge-to-join-tefca/.

11. *See generally, eHealth Exchange Network Participants*, https://ehealthexchange.org/participants/ (last accessed September 11, 2024).

12. *See ONC Draft Trusted Exchange Framework*, pgs. 3-4 (January 5, 2018), https://www.healthit.gov/sites/default/files/draft-trusted-exchange-framework.pdf.

13. *See Trusted Exchange Framework and Common Agreement*, https://www.healthit.gov/topic/interoperability/policy/trusted-exchange-framework-and-common-agreement-tefca.

14. *See Recognized Coordinating Entity Monthly Information Call*, pg. 7 (June 18, 2024), https://rce.sequoiaproject.org/wp-content/uploads/2024/06/RCE-Info-Call-June-2024_Final.pdf.

15. *See About the Recognized Coordinating Entity (RCE)*, https://rce.sequoiaproject.org/rce/.

16. *Id.*

17. *See Frequently Asked Questions, Section 5 How are QHINs Designated*, https://rce.sequoiaproject.org/rce/faqs/#WhataretherequirementstobeaQualifiedHealthInformationNetworkQHIN .

18. *See How Does TEFCA Work?*, https://rce.sequoiaproject.org/tefca/how-it-works/.

19. *See Common Agreement for Nationwide Health Information Interoperability Version 2.0* (April 2024), https://rce.sequoiaproject.org/wp-content/uploads/2024/04/Common-Agreement-v2.0_508-1.pdf.

20. *See Required Flow Down Provisions*, https://rce.sequoiaproject.org/summary-of-required-flow-down-provisions/#:~:text=TEFCA%20Exchange%20Activities%20(Section%209,to%20a%20Request%20for%20information.

21. *See Exhibit 1 to the Common Agreement for Nationwide Health Information Interoperability: Participant/Subparticipant Terms of Participation Version 1.0* (April 2024), https://rce.sequoiaproject.org/wp-content/uploads/2024/05/Common-Agreement-v2.0-Exhibit-1_508.pdf.

22. *See TEFCA Framework Exchange Purposes Explained*, https://rce.sequoiaproject.org/exchange-purposes-explained/.

23. *See Exchange Purpose (XP) Implementation SOP: Public Health Version 1.0* (August 6, 2024), https://rce.sequoiaproject.org/wp-content/uploads/2024/08/XP-Implementation-SOP-Public-Health-PH.pdf.

24. *See generally* Jim Jirjis, *CDC Office of Public Health Data, Surveillance, and Technology TEFCA Overview*, pgs. 16-22, https://www.cdcfoundation.org/TEFCADataSharingandImplementationCenters-JimJirjis.pdf?inline.

25. *See, e.g., Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing Final Rule*, 45 CFR Parts 170 & 171 (allowing providers to meet certain information blocking rule requirements by participating in TEFCA).

26. *See Meet the Designated QHINs*, https://rce.sequoiaproject.org/designated-qhins/.

27. *See supra* 11*; see also eHealth Exchange Among First to Achieve TEFCA Qualified Health Information Network (QHIN) Designation*, https://ehealthexchange.org/ehealth-exchange-among-first-to-achieve-tefca%E2%84%A0-qualified-health-information-network-qhin-designation/.

28. *See supra* 11.

29. *See Governor Hochul Announces Plans To Build a Stronger Health Care System for the Future* (January 10, 2023), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202301101.

30. *See What Is the SHIN-NY*?, https://nyehealth.org/shin-ny/what-is-the-shin-ny/.

31. *See* New York State Public Health Law §18(c)(1).

32. *See* Statewide Health Information Network for New York (SHIN-NY) Final Rule, effective July 10, 2024, https://regs.health.ny.gov/sites/default/files/pdf/recently_adopted_regulations/Statewide%20Health%20Information%20Network%20for%20New%20York%20%28SHIN-NY%29.pdf.

33. *See* CMS Waiver Authorities #11-W-00114/2, https://www.health.ny.gov/health_care/managed_care/appextension/docs/2024-01-09_ny_stc.pdf.

A New Era of Health Information Sharing Under the Information Blocking Regulations

By Christine Moundas and Gideon Palte

Over the past thirty years, regulation of health information by federal and state governments has focused primarily on establishing privacy, security, and breach notification requirements under the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA), and various state analogs. In addition, many states have passed privacy laws focused on the confidentiality and integrity of personal information, including New York's SHIELD Act[1] and the California Consumer Privacy Act as amended by the California Privacy Rights Act.[2]

While preventing health information from falling into the wrong hands remains a regulatory priority, ensuring that such information flows freely when permitted by law is now also legally required in many cases under the new federal "information blocking" regulations under 45 CFR Part 171. Noncompliance can lead to potentially significant penalties, including civil monetary penalties (CMPs) of up to $1 million per information blocking violation in certain circumstances. Health care industry stakeholders and their legal advisors should familiarize themselves with information blocking regulations to understand how their operations may be affected and to navigate a potentially active enforcement environment that is just beginning to take effect.

What Is Information Blocking?

Conceptually, the information blocking regulations create an "information sharing" mandate for certain stewards of electronic health information (EHI) – specifically, developers of federally certified health information technology ("Certified Health IT Developers"), health information exchanges and health information networks (HIE/HINs), and health care providers (collectively, "Actors") – when such sharing is legally permissible. While federal regulations specify exceptions that permit Actors not to share EHI in certain limited circumstances, the implications of this mandate stand to revolutionize the regulation of health information.

Information and technology sharing expectations under the information blocking regulations are very broad and can arise in many different circumstances. The U.S. Department of Health and Human Services (HHS), Assistant Secretary for Technology Policy and Office of the National Coordinator for Health Information Technology (ONC),[3] which is primarily responsible for information blocking enforcement along with the HHS Office of Inspector General (OIG), has provided several examples of activities that may be considered information blocking, such as the following:

- A provider notifies its electronic health record (EHR) developer of its intent to switch to another EHR system and requests a complete export of its EHI. The developer will provide the EHI only in a PDF format, even though it already can and does produce the data in a commercially reasonable structured format.
- An EHR developer requires third-party applications to be "vetted" for security before use but does not promptly conduct the vetting or conducts the vetting in a discriminatory or exclusionary manner.

- A Certified Health IT Developer takes significantly longer to provide or update interfaces that facilitate the exchange of EHI with users of competing technologies or services.
- An HIN's participation agreement prohibits entities that receive EHI through the HIN from transmitting that EHI to entities who are not participants of the HIN.
- Although not required by applicable law, a health care provider establishes an organizational policy that imposes delays on the release of lab results for any period of time in order to allow an ordering clinician to review the results or in order to personally inform the patient of the results before a patient can electronically access such results.
- A health system incorrectly claims that HIPAA rules or other legal requirements preclude it from exchanging EHI with unaffiliated providers.
- A health care provider has the capability to provide same-day access to EHI in a form and format requested by a patient or a patient's health care provider but takes several days to respond.
- A health system insists that local physicians adopt its EHR platform, which provides limited connectivity with competing hospitals and facilities. The health system threatens to revoke admitting privileges for physicians who do not comply.[4]

Potential information blocking penalties are significant, and enforcement is likely to be a priority given the federal government's investment of over $30 billion in the nation's health information technology ("health IT") infrastructure since 2009 through EHR incentive programs implemented in accordance with the Health Information Technology for Economic and Clinical Health Act of 2009 (the "HITECH Act").[5]

The 21st Century Cures Act

In December 2016, Congress passed the 21st Century Cures Act ("Cures Act"), which sought to address, among other things, information blocking concerns.[6]

In order to facilitate access to EHI when and where it is needed, the Cures Act authorizes OIG to investigate any claim that a Certified Health IT Developer, HIE/HIN, or health care provider engaged in information blocking.[7] Certified Health IT Developers, HIEs, and HINs may be subject to civil monetary penalties (CMPs) of up to $1 million per information blocking violation, and health care providers may be "referred to the appropriate agency to be subject to appropriate disincentives using authorities under applicable Federal law, as the Secretary [of HHS] sets forth through notice and comment rulemaking."[8]

In addition, the Cures Act directs the secretary of HHS to establish a prohibition on any action that constitutes information blocking as a requirement for obtaining and maintaining health IT certification under the ONC Health IT Certification Program.[9] The Cures Act also requires the secretary of HHS to establish reasonable and necessary activities that do not constitute information blocking.[10]

Information Blocking Regulations

On May 1, 2020, ONC finalized regulations codified at 45 CFR Part 171 defining "information blocking" and establishing exceptions to protect the "reasonable and necessary activities" referenced in the Cures Act (the "2020 ONC Cures Act Final Rule"). After being delayed due to the COVID-19 pandemic, these regulations took effect on April 5, 2021.[11] ONC updated these regulations in a 2024 final rule titled "Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing Final Rule" ("2024 ONC HTI-1 Final Rule").[12] ONC and the Centers for Medicare and Medicaid Services (CMS) issued a separate final rule in 2024 regarding appropriate information blocking disincentives for certain health care providers participating in the Medicare EHR Incentive Programs and the Medicare Shared Savings Program ("2024 Information Blocking Appropriate Disincentives Final Rule").[13] The 2024 Information Blocking Appropriate Disincentives Final Rule also provides that ONC will publish information blocking determinations, disincentives, and penalties that have been imposed to inform the public about how and where information blocking is occurring.[14] On August 5, 2024, ONC released a proposed rule that proposed additional changes to the information blocking regulations.[15] ONC finalized some, but not all, of these changes in final rules published in the Federal Register in December 2024.[16]

In addition, OIG issued a final rule implementing information blocking CMPs on July 3, 2023 (the "2023 OIG Information Blocking Final Rule"), with enforcement beginning effective September 1, 2023.[17]

How Is Information Blocking Defined?

45 C.F.R. § 171.103 defines information blocking as a practice that

> 1.) Except as required by law or covered by an exception set forth in the regulations, is likely to interfere with access, exchange, or use of EHI; and
>
> 2.) If conducted by a Certified Health IT Developer or HIE/HIN, such developer, network, or exchange knows, or should know, that such practice is likely to interfere with access, exchange, or use of EHI; or

3.) If conducted by a health care provider, such provider knows that such practice is unreasonable and is likely to interfere with access, exchange, or use of EHI.

What Is the Scope of EHI Subject to Information Blocking Requirements?

45 C.F.R. § 171.102 defines EHI as electronic protected health information as defined under HIPAA to the extent that it would be included in a designated record set as defined under HIPAA, regardless of whether the group of records are used or maintained by or for a covered entity as defined under HIPAA, but EHI does not include:

1.) Psychotherapy notes as defined under HIPAA; or

2.) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.[18]

Who Is Subject to Information Blocking?

45 C.F.R. § 171.102 defines the following "Actors" subject to the information blocking prohibition:

Certified Health IT Developer means an individual or entity other than a health care provider that self-develops health IT that is not offered to others, that develops or offers health IT and which has, at the time it engages in a practice that is the subject of an information blocking claim, one or more health IT modules certified under the ONC Health IT Certification Program. "Offer" is defined to exclude (1) certain health IT donation and subsidized supply arrangements; (2) certain implementation and use activities (e.g., issuing user accounts or making API technology available); and (3) certain consulting and legal services arrangements.[19]

HIE/HIN means an individual or entity that determines, controls, or has the discretion to administer any requirement, policy, or agreement that permits, enables, or requires the use of any technology or services for access, exchange, or use of EHI:

(1) Among more than two unaffiliated individuals or entities (other than the individual or entity to which this definition might apply) that are enabled to exchange with each other; and

(2) That is for a treatment, payment, or health care operations purpose, as such terms are defined under HIPAA regardless of whether such individuals or entities are subject to the requirements of HIPAA.

Health care provider includes a hospital, skilled nursing facility, nursing facility, home health entity or other long term care facility, health care clinic, community mental health center, renal dialysis facility, blood center, ambulatory surgical center, emergency medical services provider, federally qualified health center, group practice, a pharmacist, a pharmacy, a laboratory, a physician, a practitioner, a provider operated by, or under contract with, the Indian Health Service or by an Indian tribe, tribal organization, or urban Indian organization, a rural health clinic, a 340B covered entity, an ambulatory surgical center, a therapist, and any other category of health care facility, entity, practitioner, or clinician determined appropriate by the Secretary of HHS.

Information blocking requirements apply only to Actors; other types of individuals and organizations, such as health insurance plans, pharmaceutical and medical device manufacturers, and developers of technology that is not certified under the ONC Health IT Certification Program, are not subject to these requirements.

What Are the Information Blocking Exceptions?

As shown in the table below, there are ten information blocking exceptions that fall into three categories. Actors' practices that comply with all applicable requirements of an exception are not considered information blocking. Practices that do not fall within an exception are not necessarily prohibited. ONC and OIG will evaluate such practices on a case-by-case basis to determine whether information blocking has occurred.

Exception	Description	Key Conditions*
Category 1: Exceptions that involve not fulfilling requests to access, exchange, or use EHI		
Preventing Harm Exception (45 C.F.R. § 171.201)	An Actor denies access, exchange, or use of EHI to prevent harm to a patient or another person, provided certain conditions are met.	• Depending on the circumstances, the Actor must hold a reasonable belief that the practice will substantially reduce a risk of either (1) reasonably likely endangerment of the life or physical safety of the patient or another person or (2) reasonably likely substantial harm to the patient or another person; • The Actor's practice must be no broader than necessary; and • The Actor's practice must satisfy at least one condition from each of the following categories: Type of risk; Type of harm; and Implementation basis.
Privacy Exception (45 C.F.R. § 171.202)	An Actor denies access, exchange, or use of EHI in order to protect an individual's privacy, provided certain conditions are met.	The Actor's privacy-protective practice must meet at least one of the four sub-exceptions: • State or federal law precondition to EHI disclosure not satisfied; • Certified Health IT Developer not covered by HIPAA; • Denial of an individual's request for their EHI for specific "unreviewable" grounds under HIPAA; and/or • Respecting an individual's documented request not to share information.
Security Exception (45 C.F.R. § 171.203)	An Actor denies access, exchange, or use of EHI in order to protect the security of EHI, provided certain conditions are met.	• The practice must be: ◊ Directly related to safeguarding the confidentiality, integrity, and availability of EHI; ◊ Tailored to specific security risks; and ◊ Implemented in a consistent and non-discriminatory manner. • The practice must either implement a qualifying organizational security policy or implement a qualifying security determination.
Infeasibility Exception (45 C.F.R. § 171.204)	An Actor denies access, exchange, or use of EHI due to the infeasibility of the request, provided certain conditions are met.	• The practice must meet one of the following conditions: ◊ Uncontrollable events (e.g., natural or human-made disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil or regulatory authority) that in fact negatively impact the Actor's ability to fulfill the request; ◊ Inability to segment requested information from other information that cannot be disclosed by law or that is withheld under the Preventing Harm Exception, Privacy Exception or Protecting Care Access Exception: ◊ Third party seeking to modify EHI (other than a health care provider requesting modification from its business associate); ◊ Exhaustion of the Manner Exception, and the Actor does not provide the same access, exchange, or use of the requested EHI to a substantial number of individuals or entities that are similarly situated to the requester; or ◊ Infeasibility under the circumstances (as supported by a contemporaneous written record of consideration of certain factors). • The Actor must provide a written response to the requestor within 10 business days of receipt of the request with the reason(s) why the request is infeasible.

Exception	Description	Key Conditions*
Health IT Performance Exception (45 C.F.R. § 171.205)	An Actor takes reasonable and necessary measures to make health IT unavailable or degrade its performance for the benefit of the health IT's overall performance, provided certain conditions are met.	• The practice must: ◊ Last no longer than necessary; ◊ Be implemented in a consistent and non-discriminatory manner; and ◊ Satisfy additional requirements if undertaken by a Certified Health IT Developer, HIE, or HIN. • A practice targeting specific third-party apps negatively impacting health IT performance must: ◊ Last no longer than necessary; ◊ Be consistent and non-discriminatory; and ◊ Be consistent with existing service level agreements, where applicable. • Unavailability caused by risk of harm or security risks must only comply with the Preventing Harm or Security Exception, as applicable.
Protecting Care Access Exception (45 C.F.R. § 171.206)	An Actor implements a practice to reduce potential exposure to legal action related to reproductive health care, provided certain conditions are met.	• The practice must: ◊ Be undertaken based on the Actor's good faith belief that the practice could reduce the risk that persons seeking, obtaining, providing, or facilitating reproductive health care are at risk of being potentially exposed to legal action that could arise as a consequence of particular access, exchange, or use of EHI; ◊ Be no broader than necessary to reduce such risk of legal exposure ◊ Be determined based on an organizational policy or case-by-case determination that meets requirements specified in the exception;If implemented due to legal risk to a patient, affect only the access, exchange or use of specific EHI the Actor in good faith believes could expose the patient to legal action because the EHI shows, or would carry, a substantial risk of supporting a reasonable inference, that the patient: (i) obtained reproductive health care; or (ii) inquired about or expressed an interest in seeking reproductive health care; or (iii) has any health condition(s) or history for which reproductive health care is often sought, obtained or medically indicated. ◊ If implemented due to legal risk to a health care provider, affect only the access. exchange, or use of specific EHI the Actor believes could expose a provider to legal action because the information shows, or would carry, a substantial risk of supporting a reasonable inference, that they provide or facilitate, or have provided or facilitated, reproductive health care. • An Actor that is a business associate may rely on the good faith belief and determination of another Actor for which it maintains EHI as a business associate.
Category 2: Exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI		
Manner Exception (45 C.F.R. § 171.301)	This exception describes how an Actor may fulfill requests to access, exchange, or use EHI.	• An Actor may fulfill a request in any manner requested. • An Actor may use an authorized alternative manner (in order of priority: certified health IT, government or industry standards, or alternative machine readable formats) when technically unable to fulfill the request or unable to agree to terms with the requestor. Fulfillment in an alternative manner must satisfy the Fees and Licensing Exceptions, as applicable.

Exception	Description	Key Conditions*
Fees Exception (45 C.F.R. § 171.302)	This exception describes fees that an Actor may charge for fulfilling requests to access, exchange, or use EHI.	• The fees charged must meet specified requirements, including: ◊ Being based on objective and verifiable criteria that are uniformly applied; ◊ Being reasonably related to the Actor's costs and reasonably allocated; and ◊ Not being based on certain competitive factors. • Certain excluded fees are never protected: ◊ A fee for an individual's electronic access to his or her EHI; ◊ A fee for an individual's non-electronic EHI access that does not comply with HIPAA; ◊ A data export or conversion fee that was not agreed when the health IT was acquired; and ◊ A fee to export EHI using certified EHI Export technology to switch health IT or provide patients their EHI.
Licensing Exception (45 C.F.R. § 171.303)	This exception describes licensing terms that an Actor may offer to license an "interoperability element" that facilitates access, exchange, or use of EHI.	•The Actor must: Begin negotiations with the requestor within 10 business days from receipt of the request; and Finalize negotiations within 30 business days from receipt of the request. • The terms of the license must be non-discriminatory. • Any royalty charged must be reasonable. • Certain collateral terms that restrict competition (including non-competition and exclusivity provisions) are prohibited.
Category 3: Exceptions that involve practices related to Actors' participation in the Trusted Exchange Framework and Common Agreement (TEFCA)		
TEFCA Manner Exception (45 C.F.R. § 171.403)	An Actor limits the manner in which it fulfills a request for access, exchange, or use of EHI to only via TEFCA, provided certain conditions are met.	• The Actor and requestor must both be part of TEFCA. • The requestor must be capable of access, exchange, or use of the requested EHI from the Actor via TEFCA. • The request for access, exchange, or use must not be via the standards adopted for certified application programming interfaces ("APIs"). • Fulfillment of the request must satisfy the Fees and Licensing Exceptions, as applicable.

*The key conditions are not comprehensive. Please consult the applicable regulation for all requirements of an exception.

Penalties and Enforcement

Pursuant to the Cures Act, there are three enforcement mechanisms available for information blocking:

1.) Health IT certification penalties – including potential loss of health IT certification and being banned from the ONC Health IT Certification Program – enforced by ONC (applicable to Certified Health IT Developers);

2.) Civil monetary penalties of up to $1 million per violation imposed by OIG (applicable to Certified Health IT Developers, HIEs, and HINs); and

3.) Appropriate disincentives for providers participating in the Medicare EHR Incentive Programs and the Medicare Shared Savings Program, which have been implemented as follows:

a. Eligible hospitals participating in the Promoting Interoperability Medicare EHR Incentive Program would not be considered "meaningful users" of certified EHR technology (CEHRT), causing them to earn a 75% lower annual increase in Medicare payments;[20]

b. Critical access hospitals participating in the Promoting Interoperability Medicare EHR Incentive Program would not be considered "meaningful users" of CEHRT, causing them to receive 100% of reasonable costs rather than 101% of reasonable costs;[21]

c. Eligible clinicians participating in the Medicare Merit-Based Incentive Payment System (MIPS) would not be considered "meaningful users" of CEHRT, causing them to receive a score of 0 for the Promoting Interoperability MIPS Performance Category, which accounts for 25% of their MIPS score and could lead them to receive a reduction of up to 9% in Medicare payments depending on how they score against an annual benchmark specified by CMS;[22] and

d. Accountable care organizations (ACOs), ACO participants, and ACO providers/suppliers would be barred from participation in the Medicare Shared Savings Program for at least one year, after a determination by CMS that imposition of this disincentive is appropriate in light of relevant facts and circumstances (including the nature of the information blocking, the health care provider's diligence in identifying and correcting the problem, the time since the information blocking occurred, whether the provider was previously subject to a disincentive in another program, and other factors).[23]

Providers participating in the Medicare EHR Incentive Program also must attest that they do not engage in information blocking,[24] and OIG has suggested that false attestations could lead to liability under the False Claims Act, which prohibits knowingly presenting or causing to be presented a false or fraudulent claim for payment to the government.[25] In addition, OIG has explained that it will coordinate with ONC and other agencies – including the HHS Office for Civil Rights (OCR), Federal Trade Commission (FTC), CMS, and Department of Justice (DOJ) – on information blocking investigation and enforcement efforts. These agencies may impose penalties for information blocking violations that supplement the enforcement mechanisms described above. For example, information blocking that interferes with the right of access under HIPAA or involves anticompetitive conduct may lead to enforcement by OCR and FTC, respectively.

OIG has stated that it intends to create an information blocking self-disclosure process (SDP) to allow Actors to self-disclose potential information blocking violations and resolve CMP liability for conduct that constitutes information blocking, although it has not specified a timeframe for doing so. Even after the SDP is established, self-disclosure will not absolve an Actor from liability for potential consequences of information blocking violations imposed by other agencies. For example, a developer that self-discloses information blocking through the SDP could still be subject to ONC enforcement, including termination of health IT certification for its products as well as fines and penalties from OCR for practices involving violations of HIPAA requirements. Similarly, a health care provider may not escape imposition of information blocking disincentives by making an SDP disclosure.[26] Actors should carefully consider the risks of non-CMP liability against the potential benefits of self-disclosing information blocking violations to OIG, particularly given that OIG will coordinate closely with other agencies in information blocking investigations.

Pursuant to the 2024 Information Blocking Appropriate Disincentives Proposed Rule, ONC will publish on its public website certain information about Actors that have been determined by OIG to have committed information blocking, including the Actor's name, a description of the practice found to have been information blocking, the disincentives applied (if the Actor is a health care provider), and where to find additional information from the applicable government agency.[27]

Ambiguities and Potential Difficulties With State Law

The course of action that the information blocking regulations require of Actors may not be clear in all circumstances, particularly those involving potentially conflicting obligations under state law. For example, consider an individual in New York State who provides a general consent or authorization for release of his or her medical record information to a third

party, and the third party wishes to obtain HIV-related information in the individual's record from a health care provider in New York State. Under New York State law, a general authorization is not sufficient to authorize disclosure of HIV-related information.[28] Rather, an authorization specific to HIV-related information, such as pursuant to New York State Department of Health (NYSDOH) Form 2557, is required.[29]

Because the definition of information blocking excludes practices that are required by law, the health care provider may reasonably conclude that not providing the HIV-related information – as required by state law – would not be considered information blocking. However, the Privacy Exception requires an Actor that receives an authorization that is insufficient under applicable law to (a) use reasonable efforts within its control to provide the individual with a satisfactory consent or authorization form or provide other reasonable assistance to the individual and (b) not improperly encourage or induce the individual to withhold the consent or authorization. In this situation, if the denial of the request is not considered to be information blocking because the information blocking definition excludes denials that are required by law, then there should be no need for an exception. However, the additional requirements of the Privacy Exception imply that simply denying the request could be considered information blocking. In an FAQ addressing denial of requests to comply with applicable law, ONC focuses on the Privacy Exception's requirements rather than the definition of information blocking,[30] which further suggests that ONC would expect the provider to take the additional steps that the Privacy Exception requires. It remains to be seen how ONC and OIG will approach enforcement in this type of scenario.

Another example arises in the case of already established avenues for exchange of health information under state law. In particular, the new TEFCA Manner Exception established in the 2024 ONC HTI-1 Final Rule provides flexibility to Actors and requestors that participate in EHI exchange through TEFCA. However, the same flexibility is not afforded to exchange of information through state-mandated HIEs, such as the Statewide Health Information Network for New York (SHIN-NY). Most hospitals and health care facilities in New York State are required by law to participate in SHIN-NY,[31] and SHIN-NY will play a larger role in data exchange in the New York State Medicaid Program pursuant to the New York Health Equity Reform 1115 Waiver approved by CMS in January 2024.[32] However, Actors are not guaranteed that exchanging EHI through SHIN-NY will protect them from information blocking enforcement. The New York eHealth Collaborative, which is the state-designated entity charged with the governance, coordination, and administration of SHIN-NY, has previously implored ONC to adopt an information blocking exception for established HIEs such as SHIN-NY,[33] but ONC has yet to do so. It remains to be seen how ONC and OIG will regard information sharing practices of Actors that participate in state-mandated and other established HIEs when investigating information blocking allegations.

Looking Ahead

With information blocking enforcement mechanisms now in effect, the next frontier of health information regulation has arrived. ONC, OIG, and CMS are now empowered to investigate and sanction Actors that interfere with legally permissible EHI access, exchange, or use in violation of the information blocking prohibition. ONC has already received at least 1,052 possible claims of information blocking since its regulations took effect on April 5, 2021,[34] which may signal a robust forthcoming enforcement environment. Approximately 57% of these claims were submitted by patients and approximately 77% were made against providers,[35] which may suggest significant overlap with OCR's HIPAA right of access enforcement. And DOJ may regard information blocking as an additional point of leverage in investigations of Certified Health IT Developers, which have been the target of DOJ enforcement efforts in recent years.[36]

As the enforcement landscape develops, so will a clearer picture of agency priorities and possible compliance guardrails. In the interim, Actors can review the regulations and ONC's information blocking FAQs[37] to familiarize themselves with information blocking requirements. Actors may also consider taking the following proactive compliance steps:

- *Information Sharing Working Group*. Establish a cross-disciplinary working group to review information sharing practices and to identify opportunities to improve access, exchange, and use of EHI.
- *Information Blocking Compliance Policies and Procedures*. Adopt written policies and procedures that track information sharing regulatory requirements and outline a standardized approach for responding to requests to access, exchange, or use EHI.

- *Information Blocking Compliance Training*. Develop a training program to educate the workforce on the scope and requirements of the information blocking prohibition, identify requests that would be subject to the information blocking prohibition, ensure that responses to such requests are compliant, and increase awareness of escalation procedures when necessary.
- *Agreements and Forms Review*. Review agreements and forms governing the access, exchange, and use of EHI, including data use agreements, business associate agreements, interface licensing agreements, and patient release of information request and authorization forms to ensure compliance with information blocking requirements.
- *Release of EHI in Patient Portals Without Delay*. Release all EHI in patient portals without delay, unless applicable law prohibits such release or a qualifying determination of harm has been made in accordance with the Preventing Harm Exception.[38]
- *Export of EHI in Standard, Machine-Readable Formats*. Allow for the export of all EHI in standardized, machine-readable formats, such as Consolidated-Clinical Document Architecture (C-CDA) and Fast Healthcare Interoperability Resources (FHIR) formats.
- *Review of EHI Export and Interface Fees*. Actors should review any fees charged for exporting EHI or exchanging EHI through interfaces for compliance with requirements of the Fees Exception[39] and, for certified APIs, the API Condition and Maintenance of Certification requirements.[40] Developers may consider creating standard interface and data request pricing, where possible, to minimize risk that their practices are viewed as impermissibly interfering with the access, exchange, or use of EHI.

Conclusion

The information blocking regulations have ushered in a new era of health information regulation focused as much on information sharing as on privacy and security. The traditional focus on restricting inappropriate disclosures of information now has been complemented by an emphasis on ensuring that appropriate disclosures are not unduly restricted. HHS agencies are empowered to impose significant sanctions on Actors that engage in information blocking, and compliance with state information sharing requirements – such as participation in information exchange through SHIN-NY – does not guarantee information blocking compliance. Now is the time for Actors to familiarize themselves with the new requirements and bolster their compliance efforts.

Christine Moundas, a partner in Ropes & Gray's health care group and co-head of the firm's digital health initiative, provides strategic, regulatory, compliance and transactional advice to health care technology companies, health systems, pharmaceutical companies and investors. She is based in New York and can be reached at Christine.Moundas@ropesgray.com.

Gideon Palte is an associate in Ropes & Gray's health care group in New York, where he advises health care providers, technology companies, insurance companies, health care organizations and investors on transactional and regulatory issues. He can be reached at Gideon.Palte@ropesgray.com.

Endnotes

1. New York Gen. Bus. Law §§ 899-AA–899-BB.
2. Cal. Civ. Code §§ 1798.100 *et seq*.
3. ONC changed its name to "Assistant Secretary for Technology Policy and Office of the National Coordinator for Health IT" in July 2024. For simplicity and consistency, this article refers to "ONC" throughout.
4. For additional examples, s*ee* ONC, *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Proposed Rule*, 84 Fed. Reg. 7424, 7518–21 (March 4, 2019); ONC, *Information Blocking Frequently Asked Questions*, https://www.healthit.gov/faqs (last visited Nov. 14, 2024).
5. *See* Congressional Budget Office, *Answers to Questions for the Record Following a Hearing Conducted by the House Committee on the Budget: Key Design Components and Considerations for Establishing a Single-Payer Health Care System* 5 (Dec. 20, 2019), https://www.cbo.gov/system/files/2019-12/55951-CBO-QFRs.pdf.
6. Pub. L. No. 114-255 (Dec. 13, 2016).
7. *See* 42 U.S.C. § 300jj-52(b).
8. *Id.*
9. *See* 42 U.S.C. § 300jj-11(c)(5)(D)(i).
10. *See* 42 U.S.C. § 300jj-52(a)(3).
11. *See* ONC, *Information Blocking and the ONC Health IT Certification Program: Extension of Compliance Dates and Timeframes in Response to the COVID–19 Public Health Emergency Interim Final Rule*, 85 Fed. Reg. 70,064, 70,064–66 (Nov. 4, 2020).
12. 89 Fed. Reg. 1192 (Jan. 9, 2024).
13. 89 Fed. Reg. 54,662 (Jul. 1, 2024).
14. *See id.* at 54,667.
15. *See* ONC, Health Data, Technology, and Interoperability: Patient Engagement, Information Sharing, and Public Health Interoperability Proposed Rule, 89 Fed. Reg. 63,498 (Aug. 5, 2024). The changes proposed in this proposed rule have not been finalized and are not summarized in the article. For information

on the proposed changes, *see* Christine Moundas, Gideon Zvi Palte & Carolyn Lye, *ONC Proposes 'Tour De Force' Interoperability and Information Sharing Updates*, Ropes & Gray LLP (Jul. 22, 2024), https://www.ropesgray.com/en/insights/alerts/2024/07/onc-proposes-tour-de-force-interoperability-and-information-sharing-updates.

16. *See* ONC, Health Data, Technology, and Interoperability: Trusted Exchange Framework and Common Agreement (TEFCA) Final Rule, 89 Fed. Reg. 101,772 (Dec. 16, 2024), ONC, Health Data, Technology, and Interoperability: Protecting Care Access Final Rule, 89 Fed. Reg. 102,512 (Dec. 17, 2024).
17. *See* OIG, *Grants, Contracts, and Other Agreements: Fraud and Abuse; Information Blocking; Office of Inspector General's Civil Money Penalty Rules Final Rule*, 88 Fed. Reg. 42,820 (Jul. 3, 2023).
18. The 2020 ONC Cures Act Final Rule provided for an introductory period during which the scope of EHI would be limited to data elements represented in the United States Core Data for Interoperability (USCDI) Standard. This introductory period expired effective October 6, 2022, and the full EHI definition now applies. *See* 45 C.F.R. § 171.103(b).
19. 45 C.F.R. § 171.102.
20. *See* 2024 Information Blocking Appropriate Disincentives Final Rule, 89 Fed. Reg. at 54,663.
21. *See id.*
22. *See id.*
23. *See id.*
24. *See* 42 C.F.R. § 414.1375(b)(3)(ii)(A)–(C); 42 C.F.R. § 495.40(b)(2)(i)(I)(1)–(3).
25. *See* 2023 OIG Information Blocking Final Rule, 88 Fed. Reg. at 42,824. The False Claims Act is codified at 31 U.S.C. §§ 3729 *et seq*.
26. *See* 2024 Information Blocking Appropriate Disincentives Final Rule, 89 Fed. Reg. at 54,686.
27. 42 U.S.C. § 300jj–52(a)(1). *See also* 88 Fed. Reg. at 74,953–54.
28. *See* New York Public Health Law § 2782; 10 N.Y.C.R.R. § 63.5.
29. NYSDOH Form 2557 is available at https://www.health.ny.gov/forms/doh-2557.pdf.
30. ONC, *Information Blocking FAQ: Would it be information blocking if an actor does not fulfill a request to access, exchange, or use EHI in order to comply with federal privacy laws that require certain conditions to have been met prior to disclosure?* (Apr. 2023), https://www.healthit.gov/faq/would-it-be-information-blocking-if-actor-does-not-fulfill-request-access-exchange-or-use-ehi.
31. *See* 10 N.Y.C.R.R. § 300.6.
32. *See* New York eHealth Collaborative, *1115 Waiver*, https://nyehealth.org/1115-waiver/ (last visited Nov. 14, 2024).
33. New York eHealth Collaborative, *Comments to 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program - RIN 0955-AA01* p. 2 (May 28, 2019), https://downloads.regulations.gov/HHS-ONC-2019-0002-1208/attachment_1.pdf. The New York eHealth Collaborative also submitted comments to ONC regarding the TEFCA Draft 2, in which it called on ONC to explore opportunities to explicitly leverage current infrastructures, and streamline the transition for existing HIEs and HINs, in TEFCA. New York eHealth Collaborative, *Comments to Trusted Exchange Framework and Common Agreement (TEFCA) Draft 2* p. 2 (Jun. 17, 2019), https://www.nyehealth.org/wp-content/uploads/2022/02/TEFCA-Comments-6.17.19.pdf.
34. *See* ONC, *Information Blocking Claims: By the Numbers* (May 2024), https://www.healthit.gov/data/quickstats/information-blocking-claims-numbers ("ONC Information Blocking Claims Numbers").
35. *See id.*
36. Certified Health IT Developers that have been the subject of DOJ investigations include the following:

    eClinicalWorks: DOJ, Electronic Health Records Vendor to Pay $155 Million to Settle False Claims Act Allegations (May 31, 2017), https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-155-million-settle-false-claims-act-allegations.

    Greenway Health: DOJ, Electronic Health Records Vendor to Pay $57.25 Million to Settle False Claims Act Allegations (Feb. 6, 2019), https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-5725-million-settle-false-claims-act-allegations.

    Practice Fusion: DOJ, Electronic Health Records Vendor to Pay $145 Million to Resolve Criminal and Civil Investigations (Jan. 27, 2020), https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-145-million-resolve-criminal-and-civil-investigations-0.

    Athenahealth: DOJ, Athenahealth Agrees to Pay $18.25 Million to Resolve Allegations that It Paid Illegal Kickbacks (Jan. 28, 2021), https://www.justice.gov/usao-ma/pr/athenahealth-agrees-pay-1825-million-resolve-allegations-it-paid-illegal-kickbacks.

    Modernizing Medicine: DOJ, Modernizing Medicine Agrees to Pay $45 Million to Resolve Allegations of Accepting and Paying Illegal Kickbacks and Causing False Claims (Nov. 1, 2022), https://www.justice.gov/opa/pr/modernizing-medicine-agrees-pay-45-million-resolve-allegations-accepting-and-paying-illegal.
37. *See* ONC, Frequently Asked Questions, https://www.healthit.gov/faqs (last visited Nov. 14, 2024).
38. *See* 45 C.F.R. § 171.201.
39. *See* 45 C.F.R. § 171.302.
40. *See* 45 C.F.R. § 170.404.

New Technologies, New Risks: Compliance Considerations for Practitioners and Technology Companies in Remote Therapeutic Monitoring

By Scott R. Simpson

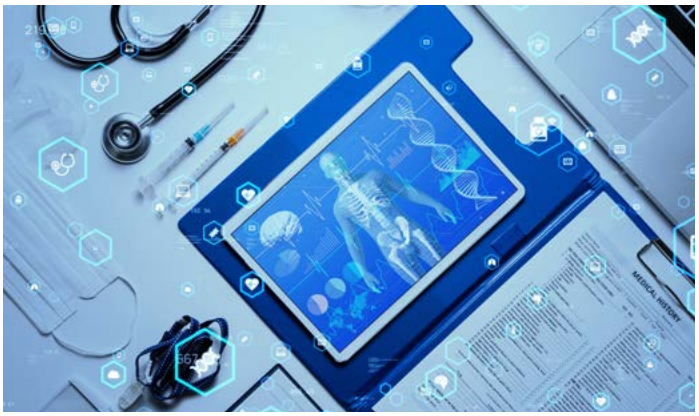
New and evolving technologies continue to present the health care industry with opportunities to improve patient outcomes and access to care and reduce the need for more expensive interventions. While reimbursement continues to be tight for orthopedic, physical therapy, and occupational therapy practices in New York, opportunities remain for New York practices that are willing to embrace these new technologies and workflows to improve both patient care and their bottom lines. Remote therapeutic monitoring (RTM) is one such area that a practice can utilize to improve patient outcomes and enhance patient engagement with the practice while generating additional revenue for the practice. However, as is often the case with new opportunities in health care, compliance pitfalls await the unwary. This article will outline these compliance concerns for practice leaders and the RTM technology companies who seek to have them as customers.

Overview of RTM

RTM involves the monitoring and collection of non-physiological data from patients by use of a Food and Drug Administration-approved connected medical device. For orthopedic and therapy practices, that data can include information on a patient's musculoskeletal system status, therapy and medication adherence, and therapy and medication response. Patients are also able to self-report data using connected medical devices and software, which is beneficial to practitioners looking to monitor patients' pain levels, tolerance to therapy, and other related data during rehabilitation.

RTM differs from remote patient monitoring (also known as remote physiologic monitoring [RPM]) in that: (1) RPM involves the collection and monitoring of physiological data,[1] (2) RPM data is reported directly by the medical device itself (whereas RTM data can be self-reported by the patient),[2] and (3) RTM CPT Codes are considered general medicine codes, which allows physical therapists (PTs) and occupational therapists (OTs) to provide and bill for RTM services.[3]

For orthopedic and therapy practices, one example of RTM is patient exercise programs that are delivered through a software application (an app). The app must be considered software as a medical device by the FDA to be eligible for use in RTM.[4] Typically, the practice enters into a licensing agreement with a technology or software company (the software company) under which the practice usually pays a per-patient monthly licensing fee to the company for use of the app. A patient's orthopedic surgeon, PT, or OT populates the app with exercises and exercise programs that the patient can perform on their own, in their own home, on their own time. The practitioner then provides the patient with credentials to access the app. The app submits data directly to the practice, some of which is provided by the patient herself. The app can be used as a complement to therapy and can even potentially replace in-person therapy with the right patient or should the patient be unable or unwilling to attend in-person therapy appointments.



A similar example of an RTM application is a web-based application that uses a camera connected or built into a laptop, tablet, or phone to track a patient's range of movement and repetitions during exercise. The application then generates a report for the patient's treating practitioner using the data collected through the use of the patient's device.

RTM gives a practitioner access to valuable data on their patients collected between visits to the office that informs the patient's rehabilitation plan.[5] That information could include pain measurements, sleep patterns, and exercise performance and technique. Given a more holistic view of their patients, practitioners can make better clinical decisions that improve patient outcomes. Additionally, for patients who (a) live in rural areas where traveling to their physician's or therapist's office is burdensome, or (b) travel often for work or other reason, RTM ensures that practitioners can keep a watchful eye on their patients' recoveries even if office visits are less frequent than they would like.[6]

The RTM CPT codes break down as shown in the chart below.[7]

CPT Code	Service	Description	Billing Frequency	Medicare Physician Fee Schedule Reimbursement[8]
98975	Initial Setup and Patient Education	Remote therapeutic monitoring (e.g., musculoskeletal system status, therapy adherence, therapy response); initial set-up and patient education on use of equipment	Once at the start of an episode	$19.65
98977	Monthly Data Transmission and Supply of Device for Monitoring (Musculoskeletal System)	Remote therapeutic monitoring (e.g., musculoskeletal system status, therapy adherence, therapy response); device(s) supply with scheduled (e.g., daily) recording(s) and/or programmed alert(s) transmission to monitor musculoskeletal system, each 30 days	Once every 30 days	$46.50
98980	Monitoring/Treatment Management Services, First 20 Minutes	Remote therapeutic monitoring treatment management services, physician/other qualified health care professional time in a calendar month requiring at least one interactive communication with the patient/caregiver during the calendar month; first 20 minutes	Once every calendar month	$49.77
98981	Monitoring/Treatment Management Services, Each Additional 20 Minutes	Remote therapeutic monitoring treatment management services, physician/other qualified healthcare professional time in a calendar month requiring at least one interactive communication with the patient/caregiver during the calendar month; each additional 20 minutes (list separately in addition to code for primary procedure)	Once every calendar month	$39.29

Since RTM remains a relatively new service, reimbursement by payors is certainly not universal. In New York, Medicare covers RTM, but Medicaid does not (at least not yet).[9] Commercial payors may or may not pay for RTM, so a review of significant payors' policies is in order before committing to an RTM program.

Fraud and Abuse Considerations

Anti-Kickback Statute

The federal Anti-Kickback Statute (the AKS) is a criminal law that prohibits the purchase, lease, or order of any good, facility, service, or item for which payment may be made by a federal health care program.[10] The AKS also prohibits giving a practitioner anything of value to refer a patient for an item or service that will be paid for by the federal government.[11] There are numerous regulatory safe harbors that protect arrangements determined by the Office of Inspector General to present a low risk of fraud and abuse.[12]

In the case of the exercise app discussed above, the Centers for Medicare and Medicaid Services (CMS) would reimburse the practitioner monthly (through CPT Code 98977) to supply the patient with access to the exercise app. The practitioner pays the software company for the use of the app. To avoid any compliance issue under the AKS, all remuneration exchanged by the practitioner and the software company should be scrutinized.

If the practitioner invests in the software company, the investment may potentially meet the requirements of the AKS safe harbor for investment interests. Regardless of whether that interest complies with all aspects of the safe harbor, it will be critical that the investing practitioner receives the same investment terms as any investor who cannot direct business

to the software company.[13] To use an extreme example, if a physician was required to put up little to no capital for the investment, but reaped significant returns, the investment returns would be highly suspect under the AKS. Further, investment terms cannot be dictated by the number of patients the practitioner can direct to use the software company's app.

For a practice to analyze a physician's investment interest in a company, the practice must know about the investment in the first instance. To avoid these types of compliance issues, practices should adopt policies that require their practitioners to disclose all investments they have, particularly the financial interests they have with any company that could or does do business with the practice.

Stark Law

The federal physician self-referral law (better known as the Stark Law) prohibits a "physician" from referring a patient for the provision of "designated health services" to an entity with which the physician has a financial relationship when those services are paid for by Medicare.[14] PTs and OTs are not included in the definition of physician.[15] Designated health services include physical therapy and occupational therapy.[16] The Stark Law has many exceptions to its general prohibition.[17] Violations are subject to significant civil penalties and can also form the basis of a claim brought under the federal False Claims Act.[18]

A physician who recommends an exercise app does not make a referral to the software company because the software company does not provide physical therapy or occupational therapy that can be billed to Medicare. Physician ownership in this type of software or device company should not be a Stark issue.

Even though the Stark Law does not prohibit a physician's ownership in a software company that she recommends to patients, RTM services are among the physical and occupational therapy codes that CMS defines as DHS. When a physician requests an advanced practice provider or other qualified practice personnel to provide the RTM services "incident to" the physician's own services, it is considered a referral under the Stark Law.[19] Some health care providers think that services billed incident to a physician's services are considered personally performed for Stark purposes, but CMS does not share that view.[20] Assuming that most providers will want to provide RTM on an incident to basis, revenue from RTM services will most likely need to be treated the same way as other DHS revenue in connection with a practice's physician compensation methodology.

Application of New York's version of the Stark Law produces the same result as in the federal context.[21] However, New York's law applies to *all* practitioners (including PTs and OTs).[22] Further, the New York statutory scheme contains a provision not contained in the federal law that requires a practitioner who refers a patient to a "health care provider" for health or health-related items or services (i.e., services not considered to be DHS by the New York law) when the practitioner has an ownership interest in the health care provider to notify the patient of the ownership interest.[23] "Health care provider" is broadly defined to include a "purveyor" of health or health-related items or services.[24] That definition is arguably broad enough to include a software company from which a practice purchases patient access to an exercise app. New York practitioners should therefore give careful consideration as to whether they are required to provide the statutory notice of any ownership interest in a software company. Statutory requirements aside, we have also seen software company licensing agreements that require disclosure of the practitioner's ownership interest to their patients.

General Risk and Compliance Considerations

To be performed most efficiently from a practice's perspective, RTM services are not performed by a physician, but by qualified practice personnel under the general supervision of a physician using Medicare's "incident to" bill construct. "General supervision" means the service is furnished under the physician's overall direction and control, but the physician's physical presence is not required during the performance of the service.[25] In PT/OT practices, RTM services can be performed by physical therapy assistants (PTAs) and occupational therapy assistants (OTAs) under the general supervision of a PT or OT, as applicable.[26] However, the Medicare program requires PTs and OTs in private practice to *directly* supervise PTAs and OTAs if the supervised PTA or OTA is not individually enrolled in Medicare.[27] Because direct supervision requires the personal presence of the PT or OT during the service performed by the PTA or OTA, from a practice perspective, that generally makes the use of non-enrolled PTAs or OTAs impractical. No matter the level of supervision required, as with any incident to service, practices should ensure that the appropriate supervision level is documented in each patient's medical record to easily demonstrate that supervision to any auditing government agency.

Orthopedic surgery practices should bear in mind that they cannot bill for RTM provided to a patient during a post-surgery global billing period. During a global billing period, all services provided by the practice to a patient that relate to the surgery (e.g., surgical follow-up visits) are not separately reimbursable from the global payment received by the practice for the surgery.[28] However, a PT practice could bill for RTM services for such a patient because the PT practice did not receive the global payment for the surgery.

Some companies that sell remote monitoring technology to practices also offer their customers documentation services

for an additional fee. These documentation services involve RTM encounter creation, note entry and encounter submission that is entered by non-licensed personnel directly into the practice's electronic health record system. This documentation forms the basis for RTM claims that the practice submits to Medicare and other payors and is the same documentation that will be audited by these payors. While these documentation services are certainly convenient, practitioners will still need to meaningfully interact with the data that comes into the EHR, both to ensure the accuracy of the patient's medical record and to make any necessary changes to the patient's treatment plan. This diligence becomes even more important when a patient uses an app or other electronic rehabilitation program as their only PT or OT program.

Once a patient has reached the goals of the care plan, the "episode of care" ceases and RTM billing should concurrently terminate.[29] While that may sound axiomatic, if the practice is not diligently monitoring the patient's data and progress, it may bill for RTM longer than is appropriate.

When a practice utilizes an app or other electronic exercise program with its patients, it is important that the patient understands their financial obligations. While there is generally no cost to the patient to use the app, an insured patient may have a cost sharing obligation in connection with the practice's RTM services. Should patients not understand that, it will at the very least generate angry calls to the practice and could invite complaints to state professional boards or the New York attorney general (even if such complaints are generally outside those regulators' jurisdiction).[30] Practices should at least discuss the financial implications to the patient and document that discussion, if not require the patient to sign an RTM consent form on which the potential for a cost-sharing obligation is disclosed in plain language.

Conclusion

Practices and RTM technology companies face several potential compliance pitfalls that must be negotiated to establish and operationalize a practice's RTM program. Practices can significantly reduce these risks by:

- Carefully evaluating agreements with software companies, especially if documentation services are part of the package the practice will purchase.
- Ensuring that patients understand how to use the technology (particularly if it will substitute for in-person rehabilitation visits) and any financial responsibility they have. Consider requiring a written patient consent form that documents the patient's understanding.
- Auditing practice personnel's review of RTM-generated data to ensure that such review actually takes place, that any red flags illuminated by the data are acted upon, and that the practice complies with RTM billing requirements.

Despite some of the compliance challenges, RTM has the potential to benefit both practitioners and patients. Practices that deploy RTM can inject some additional revenue without significant disruptions to their daily workstreams while keeping a closer eye on their patients' rehabilitation. Patients can now avail themselves of new rehabilitation platforms that will improve the quality of their care and could potentially reduce or even eliminate otherwise frequent trips for in-office therapy. Appropriate management of the compliance issues will ensure that RTM will be a valuable tool in solving some of the persistent challenges historically faced by the rehabilitation industry.

Scott R. Simpson, counsel with Nixon Peabody LLP, represents a broad spectrum of health care providers, health care companies, and private equity companies in connection with their transactional, regulatory, and compliance matters.

Endnotes

1. 86 Fed. Reg. 64,996, 65,115 (Nov. 19, 2021).
2. *Id.*
3. *Id.*
4. *Id.*
5. *See* Susan Lofton, *How Rehab Therapists Can Use RTM To Optimize Patient Care*, MedCity News, *at* https://medcitynews.com/2023/04/how-rehab-therapists-can-use-rtm-to-optimize-patient-care/#:~:text=RTM%20gives%20providers%20access%20to%20patient%20data%20and,which%20in%20turn%20reduces%20the%20chance%20of%20dropout.
6. Prabhat Sharma, *An Overview of Remote Therapeutic Monitoring*, Forbes Technology Counsel Post, Feb. 21, 2023, *at* https://www.forbes.com/councils/forbestechcouncil/2023/02/21/an-overview-of-remote-therapeutic-monitoring-rtm/.
7. 88 Fed. Reg. 78,818, 79,071-72 (Nov. 16, 2023); PYA P.C., *Providing and Billing Medicare for Remote Patient Monitoring* 14 (Feb. 2024), at https://www.pyapc.com/wp-content/uploads/2024/01/Providing-and-Billing-Medicare-for-RPM-PYA-010924.pdf.
8. The exact reimbursement rates vary by region.
9. *See* New York Medicaid Physician Fee Schedule, https://www.emedny.org/ProviderManuals/Physician/PDFS/Physician_Manual_Fee_Schedule_Sect2.xls (RTM codes are not listed).
10. 42 U.S.C. § 1320a-7b(b)(1)(B).
11. 42 U.S.C. § 1320a-7b(b)(1)(A).
12. *See generally* 42 C.F.R. § 1001.952.

13. This requirement is reflected in the "small entity investment safe harbor" at 42 C.F.R. § 1001.952(a)(2)(iii) and in OIG advisory opinions. *See, e.g.*, OIG Advisory Op. 21-18 (issued Nov. 17, 2021), available at https://oig.hhs.gov/documents/advisory-opinions/1010/AO-21-18.pdf.
14. 42 U.S.C. § 1395nn. *See also* 42 C.F.R. § 411.353(a).
15. 42 U.S.C. § 1395x(r); 42 C.F.R. § 411.351.
16. 42 U.S.C. § 1395nn(h)(6)(B)-(C); 42 C.F.R. § 411.351.
17. 42 C.F.R. § § 411.355-411.357.
18. U.S. Dep't of Health and Hum. Services, *Fraud & Abuse Laws* (last visited Sept. 8, 2024), https://oig.hhs.gov/compliance/physician-education/fraud-abuse-laws/.
19. "Incident to" services are certain services performed under the supervision of a physician but not by the physician herself. However, if the incident to billing requirements are met, the services can be billed as if they were actually performed by the physician. *See* 42 C.F.R. § 410.26; CMS, *Medicare Benefit Policy Manual*, ch. 15 § 60, *available at* https://www.cms.gov/regulations-and-guidance/guidance/manuals/downloads/bp102c15.pdf.
20. 86 Fed. Reg. 64,996, 65,350 (Nov. 19, 2021), *available at* https://www.govinfo.gov/content/pkg/FR-2021-11-19/pdf/2021-23972.pdf.
21. New York's self-referral law (N.Y. Pub. Health Law § 238 *et. seq.*) is generally less detailed than the federal analogue. New York does not define by CPT Code what is considered physical therapy like the federal Stark Law does. It is therefore not clear that RTM is considered physical therapy under the New York self-referral law. Unless a reviewing court or the Department of Health addresses the matter, it seems prudent to assume RTM is DHS for purposes of New York law.
22. N.Y. Pub. Health Law §§ 238-a(1); 238(11).
23. N.Y. Pub. Health Law § 238-d.
24. N.Y. Pub. Health Law § 238(6).
25. 42 C.F.R. § 410.26(b)(5); 84 Fed. Reg. 62,568, 62,698 (Nov. 15, 2019), *available at* https://www.govinfo.gov/content/pkg/FR-2019-11-15/pdf/2019-24086.pdf.
26. 86 Fed. Reg. 64,996, 65,115-16 (Nov. 19, 2021), *available at* https://www.govinfo.gov/content/pkg/FR-2021-11-19/pdf/2021-23972.pdf.
27. 87 Fed. Reg. 69,404, 69,642 (Nov. 18, 2022), *available at* https://www.govinfo.gov/content/pkg/FR-2022-11-18/pdf/2022-23873.pdf.
28. 88 Fed. Reg. 78,818, 78,883 (Nov. 16, 2023), *available at* https://www.govinfo.gov/content/pkg/FR-2023-11-16/pdf/2023-24184.pdf.
29. Mike Willee, *Remote Therapeutic Monitoring FAQs for PTs, OTs, and SLPs*, WebPT Blog (Apr. 8, 2022), https://www.webpt.com/blog/remote-therapeutic-monitoring-faqs-for-pts-ots-and-slps ("Code 98975 may be billed once per episode of care, which starts when the remote therapeutic monitoring service initiates and ends once targeted treatment goals are attained.").
30. Office of Professional Medical Conduct, New York State Department of Health, *Frequently Asked Questions*, at https://www.health.ny.gov/professionals/doctors/conduct/frequently_asked_questions.htm#:~:text=Generally%2C%20physician%20fees%20are%20not%20regulated%20in%20New,a%20charge%20for%20tests%20or%20services%20not%20provided%29 ("Generally, physician fees are not regulated in New York State. Complaints regarding fees are not under the jurisdiction of the Office of Professional Medical Conduct unless they represent fraud (for example, a charge for tests or services not provided).").

The State of Play for the Use of Online Tracking Technology in Health Care

By Michelle Merola

In the wake of significant push back – including litigation in the Northern District of Texas – the U.S. Department of Health and Human Services (HHS) was compelled to moderate its position on the use of online tracking technologies. Online tracking technologies are scripts or codes that collect information about users on websites or mobile apps. They have become an important part of today's digital marketplace because they allow website owners to collect data revealing how users interact with their websites. These insights inform, among other things, how businesses market services and allocate advertising resources. Although these technologies were initially implemented in the ecommerce space, today even the health care industry relies on them. As a result, HHS, which policies unauthorized disclosures of protected health information (PHI), is wading into the debate over these online tracking technologies. To understand the state of play and its implications for the future, some context is needed.

The Evolution of U.S. Privacy Law

Unlike Europe and many countries, the United States lacks a comprehensive federal privacy law. This void has resulted in a fragmented legal landscape that is composed of sector-specific federal laws and a variety of state privacy laws. In recognition of this shortcoming, federal legislators have attempted to garner support for comprehensive privacy legislation such as the American Data Privacy and Protection Act (ADPA). Modeled after Europe's General Data Protection Regulation, the ADPA, and similar proposals, would usher in regulations that address modern information-sharing and marketing tools. Until that happens, existing privacy legislation, like the Health Insurance Portability and Accountability Act of 1996 (HIPAA), is left to fill the gaps.

However, in 1996, when HIPAA entered the legislative scene, data-sharing and marketing were not, by and large, conducted via the internet. In the nearly three decades that followed, things have changed, and now the primary method of communicating with health care consumers is online. Because health care providers compete with one another for patients, digital advertising, which includes the use of online tracking technologies, is a regular and necessary component of business operations.

Commercial Surveillance Through Online Tracking Technologies

Federal agencies like the Federal Trade Commission (FTC) have long been warning consumers about the perils of commercial surveillance in the marketplace. Commercial surveillance is defined as the business of collecting, analyzing, and profiting from information about people. Tracking technologies are the cornerstone of commercial surveillance. These technologies are employed by websites and mobile apps to collect user information in various ways, often without the user's explicit awareness. Common tracking methods include cookies, web beacons and tracking pixels. Websites and mobile apps typically embed tracking code to collect mass amounts of user-provided information and device-related data, such as unique device identifiers. This data enables website and app owners or third-party vendors, such as Google Analytics, to create detailed user profiles for more accurate targeting of consumers. Website or mobile app owners may use tracking technologies developed internally or those developed by third parties. Generally, the tracking technologies developed by third parties send information directly to both the business and the third party that developed the technology. These third parties typically continue to track users and gather information about them even after they navigate away from the original website to other websites.

HHS Weighs In on Online Tracking Technologies

In the wake of guidance from the Federal Trade Commission and numerous class-action lawsuits against health care providers alleging improper disclosure of PHI, HHS' Office of Civil Rights (OCR), weighed in on tracking technologies for the first time. Specifically, in December 2022, OCR issued the first of two Bulletins (the "Original Bulletin") on the use of these online tracking technologies by HIPAA covered entities. The Original Bulletin detailed OCR's concern that covered entities had been disclosing PHI to tracking technology vendors through code placed on their websites or mobile apps. According to OCR, among the data elements being disclosed were an individual's medical record number, home or email address, dates of appointments, as well as an IP address or geographic location.

The Original Bulletin warned covered entities that under HIPAA's Privacy Rule, it is not permissible to disclose PHI to a tracking technology vendor based solely on informing individuals in a privacy policy, notice, or terms and conditions, that the covered entity plans to use these technologies. Rather, covered entities must ensure that all tracking technology vendors have signed a Business Associate Agreement and that individuals have provided HIPAA-compliant authorizations before PHI is disclosed to any vendor. Furthermore, website banners that ask users to accept or reject a website's use of tracking technologies do not constitute a valid HIPAA authorization.

To highlight the privacy concerns, the Original Bulletin also provided examples that trigger HIPAA obligations, including circumstances where an online technology connects (1) an individual's IP address with (2) a visit to an "unauthenticated public web page" addressing specific health conditions or health care providers (the "Proscribed Combination"). Unauthenticated public web pages are web pages that do not require users to log in before they are able to access the web page, such as a web page with general information about the provider like their location, visiting hours, employment opportunities, or their policies and procedures. Thus, the Original Bulletin's Proscribed Combination of IP address plus a website visit, would mean that HIPAA obligations are triggered any time a consumer navigates to a health care provider's website and does not interact with the website by providing login credentials. Covered entities and technology experts saw this example as an entirely new and unworkable obligation in the age of digital advertising.

Nonetheless, in July 2023, the FTC and HHS issued warning letters to 130 hospitals and telehealth companies about their alleged use of online tracking tools on their websites or mobile apps, stating that they were potentially violating federal data privacy and security regulations, including HIPAA. Approximately one month later, the FTC and HHS publicly named these entities and published the warning letters that were issued to the covered entities and telehealth companies. Many in the industry took issue with this public shaming because, among other things, they believed that the OCR's position on tracking technologies was overbroad in its articulation of the Proscribed Combination.

Nationwide Wave of Class Actions Related to Online Tracking Technologies

Fueled in part by the Original Bulletin from HHS, there has been a myriad of data privacy class actions across the country. Many of these lawsuits are alleging breach of state wiretapping laws, particularly in California, Pennsylvania, Florida, Illinois, and Massachusetts. Generally, wiretapping statutes in these states impose liability on any business that intercepts the contents of a user's communications without prior consent. The statutes at issue typically impose criminal liability, but also permit private civil causes of action.

For example, in California, plaintiffs' attorneys generally allege that there has been a breach of the 1967 California Invasion of Privacy Act (CIPA). CIPA lawsuits involving claims that consumer interactions have been unlawfully shared, are often designed to engender a quick settlement. However, those that have been pressed to litigation have largely been dismissed on the grounds that CIPA only applies to phone communications. Likewise, in Massachusetts, on October 24, 2024, the Supreme Judicial Court of Massachusetts weighed-in on this issue. In *Vita v. New England Baptist Hospital*, the Court rejected a plaintiff's claim that the state's Wiretap Act imposed liability on two hospitals using pixel technology on their websites. The Court reasoned that the state's analog-era wiretap statute had no application to modern pixel technology. Nevertheless, plaintiffs' attorneys continue to bring class action lawsuits under these statutes and some courts have shown a willingness to entertain these suits.

Judicial Review of HHS' Original Bulletin

As these class actions were playing out, the health care industry rallied to challenge the HHS' Original Bulletin. Specifically, two hospital associations and a regional health care system brought suit against HHS in the Northern District of Texas to stop enforcement of the Original Bulletin's Proscribed Combination. *See Am. Hosp. Ass'n v. Becerra*, __ F. Supp. 3d __, No. 4:23-cv-1110, 2024 WL 3075865 (N.D. Tex. June 20, 2024). The parties immediately moved for summary judgment and, on March 18, 2024, days before its brief was due, HHS issued a new guidance document (the "Revised Bulletin"). The Revised Bulletin softened language from the Original Bulletin, stating that it "do[es] not have the force and effect of law" and is not "meant to bind the public in any way." The Revised Bulletin further stated that "it may be prudent" for covered entities to take measures to prevent these

types of disclosures. The District Court was not persuaded, stating that,

> [T]he Privacy Rule is a mandatory legal obligation. *See* 45 C.F.R. § 164.102. Thus, it's not just "prudent" to take actions to comply with it; its legally required. While it may be prudent, it's prudent the same way it's "prudent" to drive the speed limit. No reasonable juror could read the Revised Bulletin otherwise. (*Becerra*, 2024 WL at *7.)

In its decision on summary judgment, the District Court vacated both the Original Bulletin and the Revised Bulletin to the extent they state that HIPAA obligations are triggered when online technologies connect (1) an individual's IP address with (2) a visit to an "unauthenticated public web page" addressing specific health conditions or health care providers.

Conclusion

The health care industry can claim a significant victory with the *Becerra* Court's sound reasoning, However, as the class action lawsuits demonstrate, the data-sharing and marketing controversy sparked by cookies and pixels is far from over. Moreover, as the pace of technological advances multiply, similar data-sharing boundaries will be challenged. Without comprehensive federal legislation to address these issues, the health care industry will be at the forefront of this battle to shape and interpret HIPAA's application to digital advertising.

Michelle Merola leads Hodgson Russ's Financial Institution Subpoena Compliance and Cybersecurity and Privacy Practices. She counsels clients on cybersecurity and data privacy issues under an ar-ray of international, federal, and state laws, including HIPAA, the New York State Department of Financial Services' Cybersecurity Regulation, the New York Shield Act, the California Consumer Privacy Act, and the EU's General Data Protection Regulation.

New York State Insurers' Considerations in Using Artificial Intelligence in Underwriting or Pricing

By Cassandra DiNova

The New York Department of Financial Services (DFS), which regulates insurers, issued a final Circular Letter No. 7 on July 11, 2024, titled, " Use of Artificial Intelligence Systems and External Consumer Data and Information Sources in Insurance Underwriting and Pricing" (the "Circular Letter").[1] This Circular Letter was addressed to all insurers authorized to write insurance in New York State, Article 43 corporations, health maintenance organizations, licensed fraternal benefit societies, and the New York State Insurance Fund. DFS issued this Circular Letter based on concerns for the potential discriminatory effect of external consumer data information sources (ECDIS) and artificial intelligence systems (AIS) in underwriting or pricing.

The Circular Letter outlines expectations for insurers, which can be summarized into three statements, further explained below.

1.) **Unfair or Unlawful Discrimination**. Insurers should not use ECDIS or AIS for underwriting and pricing that unfairly discriminates and should have testing in place to confirm no unfair or unlawful discrimination.

2.) **Corporate Governance and Risk Management.** Insurers need to have ECDIS or AIS incorporated into their corporate governance and risk management structures and protocols.

3.) **Disclosure to Consumers**. Insurers should disclose to consumers whether they use ECDIS or AIS in underwriting or pricing.

I. Technology Covered

Despite requests from commenters to narrow the originally proposed definitions, DFS kept its broad definitions of the applicable technology (artificial intelligence systems and external consumer data information sources) in the final Circular Letter. Below are DFS' definitions of what technology would be applicable to its Circular Letter:

> **Artificial Intelligence Systems** (AIS) means any machine-based system designed to perform functions normally associated with human intelligence, such as reasoning, learning, and self-improvement, that is used – in whole or in part – to supplement traditional health, life, property or casualty underwriting or pricing, as a proxy for traditional health, life, property or casualty underwriting or pricing, or to identify "lifestyle indicators" that may contribute to an underwriting or pricing assessment of an applicant for insurance coverage.
>
> **External Consumer Data and Information Sources** (ECDIS) includes data or information used – in whole or in part – to supplement traditional medical, property or casualty underwriting or pricing, as a proxy for traditional medical, property or casualty underwriting or pricing, or to identify "lifestyle indicators" that may contribute to an underwriting or pricing assessment of an applicant for insurance coverage. ECDIS does not include an MIB Group, Inc. member information exchange service, a motor vehicle report, prescription drug data, or a criminal history search. An insurer conducting a criminal history search for insurance underwriting and pricing purposes must comply with Executive Law § 296(16). *See e.g.*, Insurance Circular Letter No. 13 (2022).

Note, DFS' definition of AIS is not limited to generative artificial intelligence tools, but artificial intelligence in general. DFS also noted that "it is the intent of the Department to cover AIS utilization and models regardless of whether they leverage ECDIS." The Circular Letter does not provide any examples of what may be considered AIS or ECDIS. For AIS, it could be analytic or actuarial-type tools[2] and for ECDIS, it would be situations where the insurers may be acquiring or purchasing data, outside its normal course of business.

II. Unfair or Unlawful Discrimination

Put simply, insurers are still expected to follow the already existing anti-discrimination laws and need to be able to demonstrate how these tools do not violate these laws. State and federal law prohibit insurers from unlawfully discriminating against certain protected classes of individuals and from engaging in unfair discrimination, including the ability of insurers to underwrite based on certain criteria.[3] Insurers also cannot use the tools to collect or use information that it was prohibited from collecting or using directly.

Prohibitions on discrimination already existed in several regulations of the New York insurance regulations,[4] but this Circular Letter added additional requirements for insurers to prove that these tools do not discriminate. Insurers are expected to be able to demonstrate that these tools are supported by generally accepted actuarial standards of practice and are based on actual or reasonable anticipated experience, which could include statistical studies, predictive modeling, and risk assessments. DFS outlined the three steps for this anti-discrimination comprehensive assessment:

> **Step 1**: Assess whether the use of ECDIS or AIS produces disproportionate adverse effects in underwriting or pricing for similarly situated insureds or insureds of a protected class.
>
> **Step 2**: Assess whether there is a legitimate, lawful, and fair explanation or rationale for the differential effect on similarly situated insureds.
>
> **Step 3**: Conduct and appropriately document a search and analysis for a less discriminatory alternative variable(s) or methodology that would reasonably meet the insurer's legitimate business needs.

DFS recommends that insurers utilize both quantitative and qualitive methodologies for this comprehensive assessment, but insurers are not expected to collect any additional data in order to perform these assessments, only use the data it already has in its possession. Insurers are expected to perform these analyses prior to implementing these tools and whenever there is a change in their usage.

In order to do perform these assessments, insurers should have an understanding of the algorithms and methodology used by these tools, which may involve asking vendors about proprietary formulas. Insurers should determine whether they have the resources and tools to perform these assessments prior to proceeding with using ECDIS or AIS. In addition, DFS can audit an insurer's use of ECDIS or AIS, so an insurer should thoroughly document these assessments.

III. Corporate Governance and Risk Management

Insurers are already required to have a corporate governance structure,[5] and DFS states that oversight of these tools should be included in an insurer's corporate governance structure. The governing body, such as the board of directors, should have appropriate oversight of ECIS and AIS, which can be delegated to a committee. The senior management of the insurer is responsible for day-to-day implementation of these tools. DFS recommends a cross-functional management committee including representatives from legal, compliance, risk management, product development, underwriting, actuarial, and data governance.

In addition to appropriate policies and procedures, insurers should have documentation for the following as it relates to ECIS and AIS: (1) assessing the risks, (2) inventory of AIS tools, (3) description of how these tools works, (4) tracking changes of use, (5) process for monitoring, (6) testing conducted annual on output models of AIS and (7) data lifecycle management process. The Circular Letter stated that insures should be prepared to respond to consumer complaints and inquires about their ECIS or AIS usage, and make that documentation available to DFS upon request.

Insurers are expected to manage risk of its ECIS and AIS usage, which DFS adding it to insurers' already existing enterprise risk management function.[6] The Circular Letter also expected insurers to add ECIS and AIS to the items that would be internally audited by the insurer itself.[7] Insurers are also expected to have oversight of their third-party vendors' use of ECIS or AIS. DFS recommended that insurers include contract provisions for audit rights and reasonable cooperation for regulatory inquiries in vendor contracts.

IV. Disclosure to Consumers

The Circular Letter requires insurers to give notice to its consumers of its use of ECIS or AIS in underwriting or pricing. This notice should include: (i) whether the insurer uses AIS in its underwriting or pricing process; (ii) whether the insurer uses data about the person obtained from external vendors; and (iii) that such person has the right to request information about the specific data that resulted in the underwriting or pricing decision, including contact information for making such request. This notice is expected to be in advertising and marketing materials as well as during an application process.

DFS also requires an insurer using ECDIS or AIS in underwriting to provide a notice within 15 days of a determination to a denied applicant why the applicant was denied, if the applicant could have obtained insurance in a non-ECDIS or AIS underwriting process.

The challenge that insures may face with these disclosures is that "an insurer may not rely on the proprietary nature of a third-party vendor's algorithmic processes to justify the lack of specificity related to an adverse underwriting or pricing action." This means an insurer may need to provide confidentiality or other protective assurances to an AIS vendor in order to obtain the information it needs to understand how their algorithm operates in underwriting or pricing. DFS stated that failure to include both these notices may be considered unfair trade practices.

In light of this new guidance, insurers should undertake an assessment of what technologies or data they may be using for underwriting or pricing that may be considered AIS or ECDIS and evaluate how to come into compliance. Insurers should also consider creating the corporate governance structure and risk management protocols prior to using ECDIS or AIS.

Cassandra DiNova is Legal Counsel at Capital District Physicians' Health Plan, Inc. She is the Editor-in-Chief of the NYSBA Health Law Journal.

Endnotes

1. NYS Dep't of Financial Services, Circular Letter No. 7, *Use of Artificial Intelligence Systems and External Consumer Data and Information Sources in Insurance Underwriting and Pricing*, (July 11, 2024), https://www.dfs.ny.gov/industry-guidance/circular-letters/cl2024-07.
2. *See* Matthew Dobrin, Hugo Latendresse, and Adam Lewis, *Artificial Intelligence in Actuarial Science and Insurance,* Oliver and Wyman, (last accessed Nov. 11, 2024), https://www.oliverwyman.com/our-expertise/insights/2023/nov/ai-in-actuarial-science-and-insurance.html.
3. *See* Insurance Law Article 26 and § § 4224(a)–(b), 3221(q)(3), and 4305(k)(3), Executive Law, General Business Law, and federal Civil Rights Act. *See also* Insurance Law § 2303 prohibiting unfairly discriminatory rates for property and casualty insurance coverage.
4. 11 N.Y.C.R.R. § 52.72; 11 N.Y.C.R.R. § 52.75; 11 N.Y.C.R.R. § 360.5 (specific discrimination prohibition in underwriting based on sexual orientation).
5. 11 N.Y.C.R.R. § 90.1; 11 N.Y.C.R.R. § 90.2.
6. *See* Insurance Law § § 1501, 1503(b), 1604(b), 1702,and 1717(b). *See also* 11 N.Y.C.R.R. § 82.
7. 11 N.Y.C.R.R. § 89.16.

Section Committees and Chairs*

The Health Law Section encourages members to participate in its programs and to volunteer to serve on the committees listed below. Please contact the Section Officers or Committee Chairs for further information about these committees.

CLE Committee
Vacant

Diversity
Michael Fraser
N.Y.S. Unified Court System
New York, NY
mofraser@gmail.com

E-Health and Information Systems
Daniel Meier
Benesch Friedlander Coplan & Aronoff
Hackensack, NJ
dmeier@beneschlaw.com

Nathan G. Prystowsky
Johnson & Johnson
White Plains, NY
nprystowsky@icloud.com

Andria Adigwe
Buchanan Ingersoll Rooney
New York, NY
andria.adigwe@bipc.com

Ethical Issues in the Provision of Health Care
Danielle Holley Tangorre
Robinson + Cole, LLP
Albany, NY
dtangorre@rc.com

Health Care Litigation
Linda J. Clark
Barclay Damon LLP
Albany, NY
lclark@barclaydamon.com

Brian M. Feldman
Harter Secrest & Emery LLP
Rochester, NY
bfeldman@hselaw.com

Health Care Providers and In House Counsel
Margaret J. Davino
Fox Rothschild LLP
New York, NY
mdavino@foxrothschild.com

Carolyn B. Levine
Memorial Sloan Kettering
New York, NY
levinec@mskcc.org

Health Law Legislative Issues
Mark R. Ustin
Farrell Fritz, P.C.
Albany, NY
mustin@farrellfritz.com

Long-Term Care
Jane Bello Burke
Hodgson Russ LLP
New York and Albany, NY
jbburke@hodgsonruss.com

Medical Research and Biotechnology
Beth E. Roxland
The Roxland Law Firm
New York, NY
broxland@roxlandlaw.com

Membership
Salvatore Russo
Fox Rothschild LLP
New York, NY
sjrusso@foxrothschild.com

Alex Elegudin
Master of Public Health (MPH)
Candidate 2024
Columbia University Mailman School of Public Health
New York, NY
ae2746@cumc.columbia.edu

Payment, Enforcement & Compliance
William P. Keefer
Phillips Lytle LLP
Buffalo, NY
wkeefer@phillipslytle.com

Michelle Lynn Merola
Hodgson Russ LLP
Saratoga Springs, NY
mmerola@hodgsonruss.com

Professional Discipline
Douglas M. Nadjari
Ruskin Moscou & Faltischek, PC
Uniondale, NY
dnadjari@rmfpc.com

John. J. Barbera
Martin Clearwater & Bell LLP
White Plains, NY
barbej@mcblaw.com

Public Health
Heather Butts
Columbia University Mailman School of Public Health
Bayside, NY
hmbutts@aol.com

Dorothy E. Shuldman
Phillips Lytle LLP
Buffalo, NY
dshuldman@phillipslytle.com

Website/Social Media Director
Jean Denise Mancheno
Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C.
New York, NY
jdmancheno@mintz.com

Young Lawyers
Justine Lei
Sheppard Mullin
New York, NY
jlei@sheppardmullin.com

* To update your information, contact NYSBA's Member Resource Center at 1-800-582-2452 or log in at NYSBA.org

YOU ASKED. WE LISTENED. WE DELIVERED.

THE NEW YORK STATE BAR ASSOCIATION'S BRAND-NEW MEMBERSHIP MODEL IS NOW AVAILABLE!

INTRODUCING THE MOST COMPREHENSIVE AND AFFORDABLE BAR MEMBERSHIP IN NEW YORK.

RENEW OR JOIN TODAY

to start benefiting from our new model at

NYSBA.ORG/MEMBERSHIP

NYSBA®

New York State Bar Association

NEW YORK STATE BAR ASSOCIATION
HEALTH LAW SECTION
One Elk Street, Albany, New York 12207-1002

Lawyer Assistance Program

The Lawyer Assistance Program Hotline

Provided to members seeking assistance with depression, anxiety, burnout, alcohol or drug related concerns, and other mental health issues

- Free confidential service
- Up to four free counseling sessions a year

Call **877.772.8835**

NYSBA.ORG/LAP