BRACH | EICHLER LLC

Healthcare Law UPDATE

September 2020

In This Issue:

FEDERAL UPDATE

CMS Releases New Rule for COVID-19 Reporting and Testing

Centers for Medicare & Medicaid Services (CMS) released an Interim Final Rule with comment period (IFC), effective September 2, 2020, revising regulations concerning COVID-19 reporting and testing requirements for long-term care (LTC) facilities (skilled nursing facilities for Medicare and nursing facilities for Medicaid), hospitals, laboratories, physicians, and pharmacies. Noncompliance with the IFC can result in sanctions and termination from Medicare and Medicaid.

Medicare and Medicaid LTC facilities now must routinely test staff for COVID-19 and must offer testing to residents during an outbreak or if residents show symptoms. Additional guidance issued by CMS for nursing homes details the new requirements, including the testing of all staff and residents after just one new case of COVID-19 in any staff members or residents. Additionally, all staff and residents who tested negative should be retested every three to seven days for a period of 14 days since the most recent positive result. LTC facilities also must conduct routine staff testing based on the availability of Point of Service on-site testing or off-site testing with 48 hours or less turnaround time, as well as on their county's positivity rate in the prior week, now published by CMS.

The IFC also requires hospitals (short-term acute care hospitals, LTC hospitals, rehab hospitals, psychiatric hospitals, cancer hospitals and children's hospitals) and critical access hospitals to report data to the Department of Health & Human Services (HHS) on a daily basis, including the number of confirmed or suspected COVID-19 positive patients, the number of occupied ICU beds, and the availability of essential supplies and equipment.

The IFC mandates that all CLIA labs, including physician office laboratories and pharmacies, hospital laboratories, and nursing and other facilities that conduct COVID-19 testing, report test results to HHS. CMS issued additional guidance on the new requirements for CLIA labs. CLIA-certified laboratories that perform or analyze any test that is intended to detect COVID-19 or to diagnose a possible case of COVID-19, including molecular, antigen, and antibody tests, must report the results, regardless of the type of CLIA certificate held by the laboratory performing the testing. In addition, all negative and positive COVID-19 results must be reported regardless of the method used. After a three-week grace period, mandatory fines will be imposed on non-compliant CLIA-certified laboratories, of all certificate types.

In addition, the IFC allows every Medicare beneficiary to receive one COVID-19 test without a physician order; subsequent tests must be ordered by a physician or other health practitioner or pharmacist.

For more information, contact:

Riza I. Dagli | 973.403.3103 | rdagli@bracheichler.com
Joseph M. Gorrell | 973.403.3112 | jgorrell@bracheichler.com
Susan E. Frankel | 973.364.5209 | sfrankel@bracheichler.com

OCR Guidance on COVID-19-Related Plasma Donation Communications

Recovered COVID-19 patients may be able to help currently infected individuals with COVID-19 by donating their plasma. The U.S. Department of Health & Human Services, Office for Civil Rights (OCR, the HIPAA enforcement agency) released updated guidance last month to assist healthcare providers and their business associates in contacting recovered COVID-19 patients and their beneficiaries in a HIPAA-compliant manner to inquire about plasma donation.

The updated guidance updates earlier OCR guidance published in June 2020.

Under the updated guidance, a healthcare provider or health plan, or its business associate, may use protected health information (PHI) to identify and contact individuals who have recovered from COVID-19 to provide them with information about how they can donate their plasma containing antibodies to SARS-CoV-2 (the virus that causes COVID-19) for use in potentially treating patients with COVID-19. Such a use would fall under HIPAA's definition of "healthcare operations," and would not require patient authorization so long as the activity does not constitute "marketing" under HIPAA. Marketing is defined as a communication about a product or service that encourages the recipient of the communication to purchase or use the product or service, and requires patient authorization. An example of a marketing communication to patients about plasma donation would be a communication from a healthcare provider encouraging contacted individuals to use a particular blood or plasma donation center that is providing financial remuneration to the provider for such communications. An example of a non-marketing communication would be one simply providing information about plasma donation but not encouraging the use of any particular center, product, or service.

The OCR warned that disclosure of PHI to third parties for marketing communications about the third parties' products or services, such as to a blood or plasma donation center for the center's own purposes, also requires written authorization from the affected individuals.

For more information, contact:

Lani M. Dornfeld, CHPC | 973.403.3136 | ldornfeld@bracheichler.com
Joseph M. Gorrell | 973.403.3112 | jgorrell@bracheichler.com
Erika R. Marshall | 973.364.5236 | emarshall@bracheichler.com

CMS Urges States to Take Action to Facilitate Value-Based Payment

In a guidance letter to state Medicaid directors on September 15, 2020 and a related press release, Centers for Medicare & Medicaid Services (CMS) encouraged states to take action to implement value-based payments for Medicaid programs. CMS already has begun implementing various value-based payment models for the Medicare program and encourages states to use what they have learned in the process.

CMS generally lays out three recommended payment models for implementation in state Medicaid programs, each with varying degrees of deviation from the current fee-for-service payment architecture:

- Payment models built on fee-for-service architecture – direct payments on a fee-for-service basis, with (usually) retrospective adjustments for the cost and quality of services provided relative to benchmarks
- Episode of care payments – bundled payment for some or all services associated with episodes of care during a defined period of time, the amount of which may be established by comparing actual episode expenditures to an established benchmark price
- Payments involving total cost of care accountability – including bundled payments, fee-for-service, capitated payments or global payments, with healthcare providers held accountable for all populations or sub-populations for some or all services.

The underlying message is that value-based care will not happen until payers hold providers accountable through value-based payments. CMS promotes what it describes as an agile, staged approach to transform the healthcare payment landscape.

For more information, contact:

Carol Grelecki | 973.403.3140 | cgrelecki@bracheichler.com
Keith J. Roberts | 973.364.5201 | kroberts@bracheichler.com
Riza I. Dagli | 973.403.3103 | rdagli@bracheichler.com
Jocelyn Ezratty | 973.364.5211 | jezratty@bracheichler.com

ADA Expresses Concerns Regarding FTC Health Breach Notice Rule

In May 2020, the Federal Trade Commission (FTC) announced it was soliciting comments on the Health Breach Notification Rule as part of the FTC's systematic review of current FTC regulations. In general, the rule requires vendors of personal health records (PHRs) and PHR-related entities to provide: (1) notice to consumers whose unsecured individually identifiable health information has been breached; (2) notice to the media, in many cases; and (3) notice to the FTC. The rule does not apply to health information secured through technologies specified by the Department of Health & Human Services (HHS) and it does not apply to organizations covered by HIPAA. HIPAA-covered entities and their business associates instead must comply with the HIPAA breach notification rule.

On August 20, 2020, the American Dental Association (ADA) submitted a letter to the FTC containing comments to the rule. The ADA recommended that FTC and HHS work together to ensure that breach notification requirements are effective but not overly burdensome or costly to implement. The ADA cautioned that any notice requirements should not result in a patient receiving multiple or duplicative breach notices over the same incident. The ADA also expressed concern that state laws and regulations may overlap and conflict with the FTC's rule, which would be burdensome for regulated entities and could cause confusion and worry for individuals.

The comment period closed on August 20, 2020.

Other comments to the HBN Rule are posted on the Regulations.gov website.

For more information, contact:

Lani M. Dornfeld, CHPC | 973.403.3136 | ldornfeld@bracheichler.com
John D. Fanburg | 973.403.3107 | jfanburg@bracheichler.com
Cynthia J. Liba | 973.403.3106 | cliba@bracheichler.com

STATE UPDATE

New Jersey Legislative Update

Governor Murphy Signs Legislative Package to Aid LTC Facilities – On September 16, 2020, Governor Phil Murphy signed into law a series of bills designed to strengthen the resiliency and preparedness of New Jersey's long-term care (LTC) facilities to handle systemic challenges, the impact of COVID-19, and future outbreaks.

- Bill A4476/S2790 establishes certain requirements concerning the State's preparedness and response to infectious disease outbreaks, including the COVID-19 pandemic. The new law establishes the Long-Term Care Emergency Operations Center (LTCEOC) in the Department of Health (DOH), which will serve as the centralized command and resource center for LTC facility response efforts and communications during any declared public health emergency affecting or likely to affect one or more LTC facilities.
- Bill A4481/S2787 establishes the New Jersey Task Force on Long-Term Care Quality and Safety, which will be tasked with developing recommendations to make changes to the long-term system of care to drive improvements in person-centered care, resident and staff safety, quality of care and services, workforce engagement and sustainability, and any other appropriate aspects of the long-term system of care in New Jersey that the task force elects to review.
- Bill A4482/S2758 establishes minimum wage requirements for certain LTC facility staff, establishes direct care ratio requirements for nursing homes, and requires a nursing home care rate study. The law provides that the minimum wage for direct care staff in LTC facilities must be $3 higher than the prevailing NJ minimum wage, which will be annually adjusted based on cost-of-living increases. In addition, the Commissioner of Human Services will establish a direct care ratio reporting and rebate requirement whereby nursing homes will be required to report total revenues collected, along with the portion of revenues that are expended on direct care staff wages, other staff wages, taxes, administrative costs, investments in improvements to the facility's equipment and physical plant, profits, and any other factors that the Commissioner requires. The direct care ratio will require 90 percent, or a higher percentage established by the Commissioner by regulation, of a facility's aggregate revenue in a fiscal year to be expended on the direct care of residents.
- A4547/S2813 establishes a temporary rate adjustment for certain nursing facilities to support certain wage increases and to cover costs related to COVID-19 preparedness. Specifically, the law will, subject to any required federal approvals, make the reimbursement rate for certain LTC facilities equal to the rate received on September 30, 2020, plus a 10% adjustment, for the period running from October 1, 2020 through June 30, 2021. Facilities receiving the rate adjustment will be required to use at least 60 percent of the rate adjustment for the sole purpose of increasing wages or supplemental pay for certified nurse aides providing direct care. The remainder of the rate adjustment may be used for other costs related to COVID-19 preparedness and response.

Healthcare Transparency Act Passed by NJ Senate – On August 27, 2020, Bill S2465, entitled the New Jersey Healthcare Transparency Act, was passed by the New Jersey Senate and sent to the New Jersey Assembly for review. The Bill, if passed into law, would require the following:

- Advertisements of healthcare professionals (HCPs) must exclude deceptive or misleading information relating to the HCP, including, any affirmative communication or representation that misstates, falsely describes, holds out, or falsely details the professional's skills, training, expertise, education, public or private board certification, or licensure.
- HCPs must communicate, when providing in-person care, the specific professional license and professional degree the HCP holds. This information could be communicated through a name tag or embroidered identification. The name tag or embroidery must include, at a minimum, the full name of the HCP and the professional degree and professional license of the HCP. If the HCP is providing direct patient care at a hospital, the HCP would be required to wear a recent photograph, unless otherwise directed by hospital administrators.
- A poster or other signage, in sufficiently sized font, would be required to be placed at the office or offices where the HCP provides healthcare services to scheduled patients in an ambulatory setting, which must convey the professional license and professional degree held by the HCP.
- A medical doctor or doctor of osteopathic medicine who supervises or participates in collaborative practice agreements with non-physician HCPs who provides in-person patient care at the same practice location as the medical doctor or doctor of osteopathic medicine would be required to post clearly and conspicuously in each office when the medical doctor or doctor of osteopathic medicine is present.
- Medical doctors and doctors of osteopathic medicine would be prohibited from advertising or holding themselves out to the public as being board certified unless the board is a member of the American Board of Medical Specialties (ABMS) or American Osteopathic Association (AOA) or is a non-ABMS or non-AOA board that requires following certain prerequisites for issuing certification.

LTC Facility Staff Supplemental Payments Bill Passed by NJ Senate – On August 27, 2020, Bill S2788 was passed by the New Jersey Senate to provide supplemental payments to long-term care (LTC) facility staff providing direct care services during the COVID-19 pandemic. Subject to the availability of federal funds provided or made accessible to New Jersey in response to the COVID-19 pandemic, the State Treasurer would be required to establish a program to make a one-time, lump-sum payment

to any employee of a LTC facility who, during the period commencing from March 9, 2020 through the effective date of the law: (1) worked at least ten consecutive or non-consecutive weeks during which the employee provided direct care services to long-term care facility residents; (2) during each of those ten weeks, provided at least 25 hours of direct care services to long-term care facility residents; and (3) during each of those ten weeks, earned an hourly wage of less than $25 per hour or a salary that is equivalent to a wage of less than $25 per hour.

Subject to the availability of federal funds, the State Treasurer would also be required to establish a grant program for LTC facilities to provide supplemental payments to certain staff who provide direct care services at the facility. A facility would be eligible for a grant award under this program if the facility provides supplemental pay to staff members who deliver at least 25 hours of direct care services per week and who earn an hourly wage of less than $25 per hour or a salary that is equivalent to a wage of less than $25 per hour. The State Treasurer would determine the amount of the payment to be made under each program based on the total amount of available funds and the anticipated number of applicants for a payment and would establish a standardized online application process with a mechanism to verify applicant information.

For more information, contact:

John D. Fanburg | 973.403.3107 | jfanburg@bracheichler.com
Carol Grelecki | 973.403.3140 | cgrelecki@bracheichler.com
Keith J. Roberts | 973.364.5201 | kroberts@bracheichler.com
Ed Hilzenrath | 973.403.3114 | ehilzenrath@bracheichler.com

Brach Eichler **In The News**

The *New Jersey Law Journal* covered the results of the second **Brach Eichler Cannabis Poll** in an article on September 11 about conflicts between State Senators Ron Rice and Nicholas Scutari.

Managing Member and Healthcare Law Chair **John D. Fanburg** served as a panelist on the Managing Partner Forum's September 16 webinar, "Finding the Leader in You."

On October 1, **John D. Fanburg** and Labor and Employment Co-Chair **Matthew M. Collins** will host a webinar, "Recent Rule Change Requires Healthcare Providers to Offer Paid Employee Leave...What You Need to Know." To register, click here.

HIPAA CORNER - SPECIAL EXPANDED EDITION

September is National Insider Threat Awareness Month – The Cybersecurity & Infrastructure Security Agency (CISA) has announced that "September is National Insider Threat Awareness Month (NITAM), which is a collaborative effort between the National Counterintelligence and Security Center (NCSC), National Insider Threat Task Force (NITTF), Office of the Under Secretary of Defense Intelligence and Security (USD(I&S)), Department of Homeland Security (DHS), and Defense Counterintelligence and Security Agency (DCSA) to emphasize the importance of detecting, deterring, and reporting insider threats." CISA stated that NITAM 2020 will focus on "Resilience" by promoting the importance of detecting, deterring, and reporting insider threats.

Insiders are those with authorized access to an organization's resources, including personnel, facilities, information, equipment, networks, and systems. Insiders may pose security threats to organizations wittingly or unwittingly, and inflict harm through theft of proprietary information and technology; damage to company facilities, systems or equipment; actual or threatened harm to employees; or other actions that would prevent the organization from being able to carry out its normal business activities.

In order to mitigate these risks, CISA recommends that organizations establish an insider threat program, identify and protect critical assets, recognize and report suspicious behavior, and assess and respond to insider threats. Critical assets are organizational resources essential to maintaining

operations and achieving the organization's mission, such as people (employees, contractors, vendors, visitors), customers (contact and purchase information), technology (IT systems, networks, communications), confidential information (employee personal information, business sensitive or proprietary information), facilities and equipment, systems (alarm and other systems), and processes.

Uncovering and Remediating Malicious Activity – CISA issued a Joint Cybersecurity Advisory – Technical Approaches to Uncovering and Remediating Malicious Activity, dated September 1, 2020 (AA20-245A). The joint advisory is the result of a collaborative research effort by the cybersecurity authorities of Australia, Canada, New Zealand, the United Kingdom, and the United States. With the purpose of enhancing incident response and incident investigation, the report "highlights technical approaches to uncovering malicious activity and includes mitigation steps according to best practices."

Hacking: The #1 Source of Large Healthcare Data Breaches, and Probably the #1 Source for Large Penalties –

$1.5 Million Penalty for Hacking Incident – On September 21, 2020, the Department of Health & Human Services, Office for Civil Rights (OCR) announced a settlement with an orthopedic healthcare provider for alleged HIPAA violations, including a $1.5 million penalty and adoption of a corrective action plan. The allegations related to a hacking incident, in which a hacker used a vendor's credentials to access the provider's electronic medical record system for more than a month and exfiltrate patient data. According to the OCR, its "investigation discovered longstanding, systemic noncompliance with the HIPAA Privacy and Security Rules by [the provider], including failures to conduct a risk analysis, implement risk management and audit controls, maintain HIPAA policies and procedures, secure business associate agreements with multiple business associates, and provide HIPAA Privacy Rule training to workforce members." OCR Director Roger Severino stated that "[h]acking is the number one source of large healthcare data breaches." The settlement should serve as a cautionary tale to healthcare providers, both large and small, reinforcing the importance of a robust HIPAA compliance program.

$2.3 Million Penalty for Hacking Incident – On September 23, 2020, the OCR announced a settlement in the amount of $2.3 million with a business associate that provides services to hospitals and clinics of a health system, including legal, compliance, accounting, operations, human resources, information technology (IT), and health information management systems. The business associate was the victim of an Advanced Persistent Threat intrusion into its systems in 2014, pursuant to which hackers compromised administrative credentials and remotely accessed the company's information system through its virtual private network (VPN). It was determined that the intrusion affected 237 covered entity clients of the company and the hackers exfiltrated the protected health information (PHI) of over 6 million individuals. The settlement agreement closes out the OCR's allegations that the business associate violated a number of HIPAA requirements, including the requirements to (i) prevent unauthorized access to electronic PHI, (ii) respond to a known security incident and mitigate, to the extent practicable, the harmful effects of the incident, and to document the incident and its outcome; (iii) implement technical policies and procedures to allow access only to those persons or programs with access rights to information systems, (iv) implement procedures to regularly review records of system activity, such as audit logs, access reports, and security incident tracking reports, and (v) conduct accurate and thorough risk assessments. In addition to the financial penalty, the business associate agreed to a corrective action plan and monitoring for two years.

$6.85 Million Penalty for Hacking Incident Affecting Over 10.4 Million People – On September 25, 2020, the Department of Health & Human Services, Office for Civil Rights (OCR) announced a HIPAA settlement with a health insurer, including payment of $6.85 million, a corrective action plan, and monitoring. The resolution is the second-largest payment to resolve HIPAA allegations in OCR history. The breach related to a cyber attack during which hackers gained unauthorized access to the insurer's information technology system through a phishing email scheme. The access permitted an "advanced persistent threat" that was undetected for almost nine months, resulting in disclosure of more than 10.4 million individuals' protected health information being disclosed. Among the alleged HIPAA violations were a failure to conduct an enterprise-wide risk analysis and failures to implement risk management and audit controls.

OCR's Ongoing Enforcement of the HIPAA Right of Access Rule: Comply or Pay the Price of Non-Compliance – The Department of Health & Human Services, Office for Civil Rights (OCR), the HIPAA enforcement agency, announced on September 15, 2020 that it has entered into five more settlements with healthcare providers under its "Right of Access Initiative." OCR stated that its "enforcement actions are designed to send a message to the healthcare industry about the importance and necessity of compliance with the HIPAA Rules."

In a brief overview, under HIPAA, individuals have a "right of access" to the protected health information (PHI) about them held by a covered entity (e.g., a healthcare provider) in a "designated record set." Generally, a designated record of a healthcare provider includes the medical and billing records maintained for an individual, as well as other records used, in whole or in part, by the covered entity to make decisions about individuals. Covered entities must provide individuals, upon request, with access to PHI about them in a designated record set maintained by or for the covered entity. This includes the right to inspect or obtain a copy, or both, of the PHI, as well as to direct the covered entity to transmit a copy to a designated person or entity of the individual's choice. Covered entities must respond to such requests within 30 days (with certain exceptions), and may charge only a reasonable, cost-based fee for copies in paper or electronic format.

The five recent OCR settlements under the Right of Access Initiative bring the total number of enforcement actions under the initiative to seven. The recent settlements include, in addition to entering into a corrective action plan and agreeing to one or two years of monitoring by the OCR, the following:

- ***Housing Works, Inc.*** – Non-profit provider of healthcare, homeless services, advocacy, and other services agreed to pay $38,000 to settle a potential HIPAA violation based on an allegation that the provider failed to give an individual a copy of his medical records, even after the individual complained to the OCR and the OCR provided technical assistance to the provider.
- ***All Inclusive Medical Services, Inc.*** – Multi-specialty family medicine clinic agreed to pay $15,000 to settle a potential HIPAA violation based on an allegation that the clinic refused to give a patient access to her medical records when it denied her requests to inspect and receive a copy of her records.
- ***Beth Israel Lahey Health Behavioral Services*** – Network of mental health and substance-use disorder services agreed to pay $70,000 to settle a potential HIPAA violation based on an allegation that the provider failed to respond to a request from a personal representative seeking copies of her father's medical records.
- ***King MD*** – Small psychiatric healthcare provider agreed to pay $3,500 to settle a potential HIPAA violation based on an allegation that the provider failed to respond to a patient's request for access to her medical records, even after a prior OCR complaint and receipt of technical assistance from the OCR.
- ***Wise Psychiatry, PC*** – Small psychiatric healthcare provider agreed to pay $10,000 to settle a potential HIPAA violation based on an allegation of multiple failures to provide a personal representative with access to his minor son's medical records, even after a prior OCR complaint and technical assistance was provided.

Healthcare providers should take heed. The OCR has taken its Right of Access Initiative seriously, and will scrutinize complaints received by it relating to failure or refusal to provide access to patient medical records, including access to view and/or obtain copies of such records.

New OCR Health Apps Webpage – The Department of Health & Human Services, Office for Civil Rights has launched a new feature on the HHS.gov website, titled Health Apps, in order to provide resources for mobile health apps developers and "others interested in the intersection of health information technology and HIPAA privacy and security protections." Resources include Mobile Health Apps Interactive Tool; Health App Use Scenarios & HIPAA; FAQs on the HIPAA Right of Access, Apps & APIs; FAQs on HIPAA and Health Information Technology; and Guidance on HIPAA & Cloud Computing.

HHS/ONC Tool for Performing Security Rule Risk Analysis – The Department of Health & Human Services, Office for Civil Rights and the Office of the National Coordinator for Health Information Technology have released a new version of the HHS Security Risk Assessment Tool, Version 3.2 of the SRA Tool. According to the agencies, the tool is designed to assist small and medium-sized healthcare organizations to assess security risks, as required under the HIPAA Security Rule's risk analysis provisions.

If you would like assistance with your HIPAA or 42 CFR Part 2 privacy and security program, in managing or reporting a breach incident, or in business associate analysis and contracting, contact:

Lani M. Dornfeld, CHPC | 973.403.3136 | ldornfeld@bracheichler.com

BRACH | EICHLER LLC
Counsellors at Law

Healthcare Law Practice | 101 Eisenhower Parkway, Roseland, NJ 07068

Members

Riza I. Dagli | 973.403.3103 | rdagli@bracheichler.com
Lani M. Dornfeld, HLU Editor | 973.403.3136 | ldornfeld@bracheichler.com
John D. Fanburg, Chair | 973.403.3107 | jfanburg@bracheichler.com
Joseph M. Gorrell | 973.403.3112 | jgorrell@bracheichler.com
Carol Grelecki | 973.403.3140 | cgrelecki@bracheichler.com
Keith J. Roberts | 973.364.5201 | kroberts@bracheichler.com

Counsel

Shannon Carroll | 973.403.3126 | scarroll@bracheichler.com
Debra W. Levine | 973.403.3142 | dlevine@bracheichler.com
Jonathan J. Walzman | 973.403.3120 | jwalzman@bracheichler.com
Edward J. Yun | 973.364.5229 | eyun@bracheichler.com

Associates

Colleen Buontempo | 973.364.5210 | cbuontempo@bracheichler.com
Lindsay P. Cambron | 973.364.5232 | lcambron@bracheichler.com
Paul J. DeMartino, Jr. | 973.364.5228 | pdemartino@bracheichler.com
Jocelyn E. Ezratty | 973.364.5211 | jezratty@bracheichler.com
Susan E. Frankel | 973.364.5209 | sfrankel@bracheichler.com
Ed Hilzenrath | 973.403.3114 | ehilzenrath@bracheichler.com
Cynthia J. Liba | 973.403.3106 | cliba@bracheichler.com
Erika R. Marshall | 973.364.5236 | emarshall@bracheichler.com

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