

BRACH | EICHLER<sup>LLC</sup>  
Counsellors at Law



JAN | 2022

# 2021 Healthcare Law Year in Review

BB  
|  
FF

---

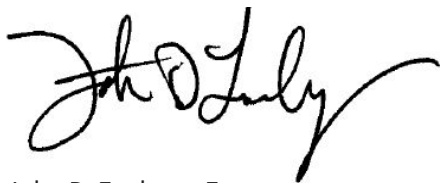
Happy New Year! We are pleased to introduce our 13th annual *Healthcare Law Year in Review* produced by the Brach Eichler Healthcare Law Practice. The goal of this publication is to highlight some of the most important issues and developments in healthcare, both nationally and in New Jersey, over the past 12 months.

Looking back to this time last year, the only positive thing any of us could say about the year 2020 was that it was behind us. In 2022, we now find ourselves in a far better and more hopeful place. Undoubtedly, the pandemic has not been defeated – in fact, at this moment we are all processing the potential impact of the latest Omicron variant – however, the global vaccine push has eased our return to a more familiar routine.

As we begin 2022, we continue to expect to see a significant shift in healthcare policy. Among the issues covered in this year's report are:

- COVID Response, Expansion, and Vaccination/Booster Mandates
- Prescription Drug Pricing, Surprise Billing, and Value-Based Care
- Massive Expansion in Telehealth and Regulations
- Stark and Anti-Kickback Reform
- Healthcare Transformation and Deal Trends

As always, Brach Eichler's healthcare law attorneys are available to provide guidance and/or assist with mergers and acquisitions, labor and employment, contracts and agreements, and any other legal matters. If you have any questions or would like additional information regarding any of the articles contained in the 2021 Healthcare Law Year in Review, please do not hesitate to contact us. Thank you for your continued support. Be well, be safe.



John D. Fanburg, Esq.  
Managing Member and Chair, Healthcare Law Practice  
Brach Eichler LLC  
973-403-3107  
jfanburg@bracheichler.com



Lani M. Dornfeld, Esq., CHPC  
Member, HLU Editor  
Brach Eichler LLC  
973-403-3136  
ldornfeld@bracheichler.com

---

## FEDERAL UPDATE

### The Federal “No Surprises Act” and Related Regulations Prohibiting Surprise Medical Bills Come Into Effect January 1, 2022



On December 27, 2020, President Donald Trump signed into law the “[No Surprises Act](#)” (NSA) to protect American consumers against excessive out-of-pocket costs due to surprise medical bills and balance billing by certain healthcare providers. During 2021, multiple federal agencies published regulations to implement the new federal law. On July 13, 2021, the Department of Health and Human Services (HHS), the Department of Labor, the Department of the Treasury, and the Office of Personnel Management published the “[Requirements Related to Surprise Billing; Part I](#)” interim final rule, and on September 30, 2021, they issued the “[Requirements Related to Surprise Billing; Part II](#)” interim final rule. Effective January 1, 2022, the NSA provides, among other things, the following protections for insured and non-insured individuals.

#### Insured Individuals – Protection from Balance Billing

For people who have health coverage through an employer, a Health Insurance Marketplace, or an individual health plan purchased directly from an insurer, the NSA:

- Bans surprise bills for emergency care services by out-of-network (OON) providers or OON emergency facilities, and requires that cost sharing for these services (e.g., co-pays)

be based on in-network rates, even when care is received without prior authorization.

- Bans surprise bills for covered non-emergency care services, including stabilization services, by certain OON providers at in-network facilities (hospitals, hospital outpatient departments, and ambulatory surgical centers).
- Bans surprise bills for air ambulance services by OON air ambulance providers.
- Requires providers and facilities to share with patients easy-to-understand *notices* that explain the applicable billing protections and who to contact if they have concerns that a provider or facility has violated the new surprise billing protections. The form of the notice designed by HHS is available [here](#). Providers must use the form in its original format; no edits permitted.
- Permits OON providers and facilities to obtain *waivers* from insured patients to permit balance billing under certain circumstances, but prohibits waivers for ancillary services such as anesthesia, pathology, radiology, neonatology, and the services of hospitalists, intensivists, and assistant surgeons.
- Establishes the federal independent dispute resolution (IDR) process that OON providers, facilities, providers of air ambulance services, plans, and issuers in the group and individual markets may use to determine the OON rate for applicable items or services after an unsuccessful open negotiation.
- Does not apply to Medicare, Medicaid, Indian Health Services, Veterans Affairs Health Care, or TRICARE.

### **Non-Insured and Self-Pay Individuals – Right to Advanced Knowledge of Costs**

For people who do not have health insurance or those who desire to pay for care on their own, the NSA:

- Requires most providers to give a *good faith estimate* of costs before providing non-emergency care.
- Requires the good faith estimate to include expected charges for the primary item or service, as well as any other items or services that would reasonably be expected. For example, when getting surgery, the estimate must include the cost of the surgery, as well as any labs, tests, and anesthesia services that might be used with the procedure. However, other items or services related to the surgery that might be scheduled separately, like pre-surgery appointments or physical therapy in the weeks after the surgery, do not have to be disclosed in the good faith estimate.
- Provides a model notice, “The Right to Receive a Good Faith Estimate of Expected Charges” and a “Good Faith Estimate Template” to be provided to all uninsured and self-pay patients. The notice and good faith estimate template can be found [here](#).
- Provides a specific timeframe for giving the good faith estimate to patients.

- Provides a process for patients to dispute final charges that exceeds the good faith estimate by \$400 or more.

### **Remedies**

The NSA and the detailed regulations promulgated thereunder are effective January 1, 2022. Providers and facilities must ensure compliance to avoid complaints, citations and civil monetary penalties up to \$10,000. Miscellaneous information and fact sheets are available [here](#). Providers can file a complaint against health plans they believe are not complying with the NSA [online](#) or by calling 1-800-985-3059. Consumers can find information about the NSA, initiate a payment dispute and submit complaints directly on the [CMS website](#).

### **Interplay Between the NSA and New Jersey’s Out-of-Network Law**

Implementation of the NSA is complicated in New Jersey due to the fact that New Jersey has its own law governing out-of-network billing. New Jersey’s “[Out-of-Network Consumer Protection, Transparency, Cost Containment and Accountability Act](#)” (the NJ OON Law) became effective in August of 2018. Like the NSA, the NJ OON Law provides notice requirements, balance billing limitations and an arbitration procedure for out-of-network claims that are covered by the law. However, the NJ OON Law is not consistent with the NSA in all respects.

Often when federal and state law conflict, federal law preempts state law. In the interplay between the NSA and the NJ OON Law, this is not always the case. In this case, the NSA creates a “floor” of protections against surprise bills from out-of-network providers, but does not preempt state laws that provide at least the same or greater protections against surprise bills and higher cost-sharing as is provided by the NSA. Therefore, because the NSA has, to a large extent, more stringent notice and consent requirements than the NJ OON Law, providers will be required to use the federal notice forms when applicable. However, because the NJ OON Law does require that certain disclosures be made beyond what is required in the NSA, when the NJ OON Law is applicable, providers will be required to make both federally mandated disclosures and New Jersey required disclosures.

Moreover, with respect to arbitration, so long as a state’s dispute resolution process meets or exceeds the minimum requirements under the federal IDR, HHS will defer to the state process. New Jersey’s dispute resolution process appears to meet or exceed the federal requirements. Therefore, New Jersey’s dispute resolution process will take precedence over the federal IDR for matters that are within the jurisdiction of New Jersey’s process. This includes matters that arise from claims for services rendered to patients that are covered under New Jersey licensed health benefit plans. The New Jersey process does not, however, apply to disputes that arise from claims for services rendered to patients that are covered under the Federal Employees Health Benefit Program, or self-funded plans (i.e., ERISA plans) that do not opt into the New Jersey process. These disputes would need to proceed under the federal IDR.

---

## Expansion of the Home Health Value-Based Purchasing Model

---

Centers for Medicare & Medicaid Services (CMS) [announced](#) on January 8, 2021 its intention to expand the Home Health Value-Based Purchasing (HHVBP) model first implemented by the CMS Innovation Center in January of 2016. This model was first implemented in order to determine if Medicare beneficiaries would receive improved home healthcare services if CMS were to provide payment incentives for better quality of care with greater efficiency rather than payments based on the volume of services. The CMS Innovation Center has had nine states, Arizona, Florida, Iowa, Maryland, Massachusetts, Nebraska, North Carolina, Tennessee, and Washington, participate in the model thus far. Pursuant to Section 1115A(c) of the Social Security Act, the Secretary of Health and Human Services (the Secretary) via rulemaking may expand the duration and scope of a model test if it meets the following requirements: (i) it is determined that such an expansion is expected to reduce spending without reducing the quality of care or improve the quality of patient care without increasing spending; (ii) the Chief Actuary of CMS must certify that such expansion would reduce (or would not result in any increase in) net program spending; and (iii) the Secretary must also ensure that such an expansion would not deny or limit the coverage of benefits. It has been determined that the HHVBP model meets these requirements. Based on the data from 2016-2018, the HHVBP model demonstrated improved quality of care without causing significant provider burden or adverse effects on patient access and reduced the number of unplanned hospitalizations. This model showed an average annual savings of [\\$141 million](#) to Medicare.

The expansion of the HHVBP model is being implemented through CMS regulations and began January 1, 2022, with calendar year 2022 as a pre-implementation year.

---

## What's in a Name? OIG Updates Its Health Care Fraud Self-Disclosure Protocol

---

On November 8, 2021, the Office of Inspector General (OIG) for the U.S. Department of Health & Human Services (HHS) renamed and updated its process for a party to voluntarily identify, disclose, and resolve instances of potential fraud involving federal healthcare programs. The OIG's prior Self-Disclosure Protocol is now known as the *Health Care Fraud Self-Disclosure Protocol* (the "Protocol"). More than just a name change, the OIG updated several parts of the Protocol, including:

- Requiring the disclosing party to include whether it is subject to a corporate integrity agreement (CIA). If so, the disclosing party must also send a copy of the voluntary disclosure to its CIA monitor.
- Requiring voluntary disclosures relating to an HHS grant or contract to be submitted to the OIG's separate grant self-disclosure program or contractor self-disclosure program.

- Requiring voluntary disclosures to be made online at the [OIG's website](#). The online form allows for a party to submit attachments after submitting the form.
- Requiring voluntary disclosures to include the damages amount for each affected federal healthcare program and the sum of all damages for all affected federal healthcare programs.
- Increasing the minimum amount required to settle matters to \$20,000 for false claims and \$100,000 for anti-kickback-related conduct, which is consistent with recent legislative changes.

The OIG did not update other parts of the Protocol, including the methodology for calculating damages.

From 1998 to 2020, over 2,200 parties have made voluntary disclosures resulting in the OIG recovering over \$870 million.

---

## Federal Bill Would Require Ransomware Victims to Disclose Ransom Payments to the Government

---

On October 5, 2021, Senator Elizabeth Warren and Representative Deborah Ross [introduced](#) a federal [bill](#) that would, if passed into law, require victims of ransomware attacks to disclose to the Department of Homeland Security (DHS) ransom payments made to cyber attackers.

If passed into law, the "Ransom Disclosure Act" would:

- Require ransomware victims (excluding individuals) to disclose information about ransom payments no later than 48 hours after the date of payment, including the dates and amount of ransom demanded and paid, the type of currency used for payment of the ransom, any known information about the entity demanding the ransom, and whether the victim that paid the ransom receives federal funds.
- Require DHS to make public the information disclosed during the previous year, excluding identifying information about the entities that paid ransoms.
- Require DHS to establish a website through which individuals can voluntarily report payment of ransoms.
- Direct the Secretary of Homeland Security to conduct a study on commonalities among ransomware attacks and the extent to which cryptocurrency facilitated these attacks and provide recommendations for protecting information systems and strengthening cybersecurity.

---

## DOJ Announces Charges in \$1.4B Fraud Scheme, Including by Use of Telemedicine

---

On September 17, 2021, the U.S. Department of Justice (DOJ) announced criminal charges against 138 defendants, including 42 doctors and other healthcare providers in 31 federal districts across the country, alleging participation in

---

various healthcare schemes resulting in approximately \$1.4 billion in alleged losses.

The largest target is fraud committed using telemedicine, in the amount of approximately \$1.1 billion, resulting from allegedly false and fraudulent claims submitted by more than 43 defendants. Allegations include telemedicine executives paying doctors and nurse practitioners to order unnecessary durable medical equipment (DME), genetic and other diagnostic testing, and pain medications either without any patient interaction or with only a brief telephonic conversation with patients the providers had never met or seen. DOJ alleges that DME companies, genetic testing laboratories, and pharmacies then purchased those orders in exchange for illegal kickbacks and other bribes and submitted false and fraudulent claims to Medicare and other government payers. Allegations also included “sham” telemedicine consultations. DOJ alleges the kickbacks and other monies received were used to purchase luxury items such as vehicles, yachts, and real estate.

COVID-19 fraud cases totaling over \$29 million are alleged against nine of the defendants. Allegations include exploiting policies put into place by Centers for Medicare & Medicaid Services to increase access to care during the COVID-19 pandemic, such as expanded telehealth regulations. Charges include misuse of patient information to submit claims to Medicare for unrelated laboratory testing that was expensive and unnecessary, including cancer genetic testing. Also targeted were sober homes, including allegations of over \$133 million in false and fraudulent claims for tests and treatments relating to drug and alcohol addiction. Nineteen defendants were charged with illegal prescription and/or distribution of opioids, with over \$14 million in false billings.

---

## Physician Owner of ASC May Profit from Employed CRNA's Services at ASC

---

The Office of Inspector General (OIG) of the Department of Health & Human Services determined in [Advisory Opinion No. 21-15](#) that a pain management practice solely owned by a physician and the ambulatory surgery center (ASC) at which the physician is a majority owner may profit from anesthesia services performed by the practice's employed certified registered nurse anesthetist (CRNA) in the practice office and at the ASC. The OIG concluded that it would not impose sanctions under the federal anti-kickback statute relating to the proposed arrangement.

Under the federal anti-kickback statute, it is a criminal offense to knowingly and willfully offer, pay, solicit, or receive any remuneration to induce, or in exchange for, referrals reimbursable under a federal healthcare program. “Remuneration” includes the transfer of anything of value, directly or indirectly, in cash or in kind. The statute has been interpreted to cover any arrangement where one purpose of the remuneration is to induce referrals. The statute and its regulations provide safe harbors, or exceptions, that set forth specific arrangements that do not violate the law. One safe harbor applies to compensation paid to a bona fide employee.

Under the arrangement described in the advisory opinion, the pain management practice pays a salary to the employed CRNA, who provides anesthesia services in the practice's office and at the ASC. Under the CRNA's employment agreement, the CRNA reassigned to the practice the right to receive reimbursement for the separately-billable anesthesia services performed by the CRNA, whether in the medical office or in the ASC. The practice bills for all of the CRNA's anesthesia services provided in both settings. The practice also assumes responsibility for the CRNA's performance of



anesthesia services. The OIG determined that, because the CRNA is a bona fide employee of the practice, the salary to the employee is not a kickback. The OIG further found that although the reassignment of benefits flows from the employee to the employer, and technically is not protected by the anti-kickback statute's employee safe harbor, the arrangement is not a kickback scheme, because salaries to bona fide employees in exchange for reassignment of benefits are (i) a common practice in the healthcare industry, and (ii) are explicitly authorized by the Medicare program.

---

## EHR Developer Pays \$3.8 Million to Settle Kickback Claims

---

CareCloud Health, Inc. f/k/a CareCloud Corporation (CareCloud), a developer of electronic health records (EHR), agreed to pay [\\$3.8 million to settle](#) claims by the federal government that it paid unlawful kickbacks to promote its EHR products.

By way of background, in 2017, a former senior manager at CareCloud filed a [federal qui tam](#), or whistleblower, action alleging, among other claims, that CareCloud paid kickbacks to clients to promote their services. As a result, the whistleblower alleged, the program violated the federal Anti-Kickback Statute and False Claims Act (FCA). The United States reviewed the whistleblower's claims and decided to prosecute the case against CareCloud. The United States alleged that CareCloud gave existing clients cash equivalent credits, cash bonuses, and success payments to recommend its services to potential new clients. In addition, clients participating in the incentive program were prohibited from giving negative information about CloudCare to potential clients.

---

The whistleblower will receive \$803,269.97 for bringing the original lawsuit. The whistleblower got the idea to bring a lawsuit by reading about a previous settlement of \$155 million by EHR vendor eClinicalWorks. These settlements are a reminder to all in the healthcare industry to maintain a robust compliance program, including addressing marketing efforts.

## STATE UPDATE

### New Jersey Non-Profit Hospitals Must Make Community Service Payments to Retain Property Tax Exemption

On February 22, 2021, Governor Murphy signed into [law](#) legislation that allows non-profit hospitals, as well as satellite emergency care facilities owned by hospitals, to retain their property tax exemption while they are assessed an annual community service contribution to be paid to the municipality in which the hospital or facility is located.

The law addresses a 2015 Tax Court [ruling](#) which found that Morristown Medical Center, a tax-exempt non-profit corporation, did not meet the legal standard to be a non-profit due to its web of non-profit and for-profit activities and, therefore, was not exempt from property taxation. The Tax Court also found that if other non-profit hospitals operated similarly, their non-profit status was a “legal fiction” and they too should be subject to property taxation. The court explained that it was up to the legislature to clarify the terms and conditions for property tax exemption.

Under the new law, for tax year 2021, non-profit hospitals must pay \$3.00 per day for each licensed bed at the hospital, and satellite emergency care facilities must pay \$300 per day. The per-day amount will increase by two percent in each subsequent tax year. If any portion of a hospital or satellite emergency care facility property is leased to a for-profit organization or is otherwise used for purposes that are not tax-exempt, that portion of the property is subject to property taxation. The law allows hospitals to seek an exemption from the community service contribution if the hospital did not bill in the previous year any patient for inpatient or outpatient professional or technical services provided at the hospital, and if the hospital provided community benefits over the prior three years averaging at least twelve percent of the hospital’s total expenses. Hospitals and facilities may also reduce the required contributions by any amounts paid to municipalities under voluntary agreements.

---

### DOBI Data on Out-of-Network Arbitrations is Positive For Providers

As most New Jersey providers are aware, the New Jersey Out-of-Network Consumer Protection, Transparency, Cost Containment, and Accountability Act (P.L.2018, c.32) (Act), which took effect on August 30, 2018, prohibits providers from balance billing a covered person for inadvertent out-of-

network services and/or out-of-network services provided on an emergency or urgent basis above the amount of the covered person’s liability for in-network cost-sharing. The Act established an arbitration process to resolve out-of-network billing disputes between providers and insurance carriers (and self-funded plans that opt in to the arbitration provisions of the Act) for inadvertent and/or emergency/urgent out-of-network services. The New Jersey Department of Banking and Insurance (“DOBI”) released [data](#) on January 31, 2021 detailing the status of arbitrations commenced under the Act for calendar year 2020, and the results are encouraging for providers.

As of December 31, 2020, MAXIMUS Federal, the DOBI contractor handling arbitrations under the Act, had received 5,715 arbitration requests, of which 4,173 were resolved by decision, 813 were dismissed as ineligible, and 729 cases were withdrawn. Of the 4,173 arbitration awards issued, providers prevailed in 2,683 cases or 64% of the total, while insurance carriers prevailed in 1,489 cases or 36% of the total. Providers were awarded \$31.4 million, while awards to carriers were \$5.2 million. Of the cases that were dismissed as ineligible, the primary reasons for dismissal were that the health benefits plan was issued in a state other than New Jersey or the plan was a self-funded plan that did not opt into arbitration. Further details on each arbitration filed can be found [here](#).

Also noteworthy is that between January 1, 2020 and December 31, 2020, DOBI received just 76 consumer complaints relating to out-of-network healthcare charges.

The takeaway from this data is that providers should not be discouraged from pursuing arbitration if they dispute a carrier’s or plan’s fee for out-of-network inadvertent or emergency/urgent services.

## NEW JERSEY LEGISLATIVE UPDATE

### New Law Revises Requirements for Insurers to Cover Telemedicine Services

On December 21, 2021, Governor Murphy signed into law former [Bill S2559](#), which revises certain requirements for health insurance providers covering telemedicine and telehealth. Carriers offering health benefit plans in New Jersey, the State Medicaid and NJ FamilyCare programs, the State Health Benefits Program, and the School Employees’ Health Benefits Program (Programs), are now prohibited from imposing any restrictions on the location or setting used by a healthcare provider to provide services using telemedicine and telehealth or on the location or setting of where the patient is located when receiving services using telemedicine and telehealth, so long as the services provided using telemedicine and telehealth meet the same standard of care as if the services were provided in person. In addition, such Programs are now prohibited from restricting the ability of a provider to use any electronic or technological platform to provide services using telemedicine or telehealth, provided that the platform allows the provider to meet the same standard of care as would be provided if the services were provided in person.

---

## Audiologists Permitted to Dispense and Fit Hearing Aids

---

Effective May 17, 2021, the New Jersey Division of Consumer Affairs adopted [amendments](#) to the audiology regulations to expand the scope of practice of licensed audiologists to include dispensing and fitting hearing aids. New Jersey law permits licensed audiologists to dispense and fit hearing aids, as long as the audiologist has completed coursework and



clinical training in the dispensing and fitting of hearing aids that meet the requirements established by the Division of Consumer Affairs Audiology and Speech-Language Pathology Advisory Committee (Committee). The Committee reviewed the educational programs for audiologists and determined that all such education programs contain content that prepares graduates to dispense and fit hearing aids.

---

## Nurse Licensure Compact Regulations Adopted

---

Effective May 17, 2021, the New Jersey State Board of Nursing adopted [regulations](#) to implement P.L. 2019, c. 172, which entered New Jersey into the Nurse Licensure Compact (Compact). The Compact is an agreement among states in which nurses licensed in one member state (home state) may work in another member state (remote state) without obtaining a license in the remote state. To work in a remote state, a nurse would have to obtain a license with multistate privileges from his or her home state, which must be the nurse's primary state of residence. To effectuate the Compact, the Board of Nursing adopted amendments to its existing rules and established new rules and procedures for applying for licenses with multistate privileges. The Interstate Commission of Nurse Licensure Compact Administrators recognizes that applicants for certification as advanced practice nurses or forensic nurses-certified sexual assault (FN-CSA), who are licensed as registered professional nurses to obtain certification, must meet the licensure requirement by holding a license with multistate privileges in a remote state.

---

## New Law Requires Healthcare Facilities to Report COVID-19 Data

---

On February 4, 2021, Governor Phil Murphy signed into law [Bill S2384/A4129](#) to require healthcare facilities to report certain coronavirus disease 2019 (COVID-19) data related to healthcare workers and certain first responders. Specifically, general acute care hospitals, special hospitals, ambulatory care facilities, ambulatory surgical centers, assisted living facilities, home health agencies, nursing homes, and hospice programs are required to report to the Department of Health (DOH) either directly or through a non-profit trade association, on a bi-monthly basis, de-identified data on the number of healthcare professionals, ancillary healthcare workers, and emergency medical services personnel employed by the facility who tested positive for COVID-19 and who died from COVID-19. The DOH will be required to issue a report concerning the occupational data received pursuant to the new law no later than 12 months after the end of both the state of emergency and public health emergency declared in response to the COVID-19 pandemic.



---

## HIPAA Highlights

**Safe Harbor for Implementation of “Recognized Security Practices”** – On January 5, 2021, the Health Information Technology for Economic and Clinical Health (HITECH) Act was [amended](#), creating a “safe harbor” for HIPAA covered entities and their business associates when potentially facing fines and other penalties under HIPAA. If the covered entity or business associate can “adequately demonstrate” to the Secretary of the U.S. Department of Health and Human Services (DHHS) that it had “recognized security practices” in place for at least the twelve month period prior to the conduct in question—HIPAA violation, breach event or audit—the Secretary may determine to mitigate any fines to be assessed, favorably terminate early an audit that has been undertaken, or mitigate the remedies in any settlement agreement that may be entered into between the covered entity or business associate and the government. In short, a covered entity or business associate

that has experienced a data breach incident and is responding to the related DHHS investigation and document requests, or is otherwise under a HIPAA audit, may be able to assert this safe harbor to reduce or eliminate fines and penalties. These recognized security practices must be consistent with industry standards including those set forth in [Section 2\(c\)\(15\) of the National Institute of Standards and Technology \(NIST\) Act](#) and those described in [Section 405\(d\) of the Cybersecurity Act of 2015](#). The practices, among other things, must address the “5 top Threats” to cybersecurity—email phishing, ransomware, loss or theft of equipment, insider, accidental or intentional data loss, and attacks against medical devices—by implementing “10 Best Practices” to manage these threats.

**White House Urges Businesses to Protect Against the Threat of Ransomware** – On June 2, 2021, Annie Neuberger, Deputy Assistant to the President and Deputy National Security Advisor for Cyber and Emerging Technology, released a [memo](#) urging businesses to take steps to protect themselves against the threat of ransomware. This is in response to the number and size of recent ransomware incidents in the United States and around the world. The memo addresses the critical responsibility the private sector has in protecting against these threats.

According to the memo, these immediate steps will help protect businesses, their customers or consumers, and the broader economy:

- Implement the five best practices from the [President’s Executive Order](#); this includes:
  - Multifactor authentication;
  - Endpoint detection and response;
  - Encryption; and
  - A skilled and empowered security team.
- Back up your data, system images, and configurations, regularly test them and keep the backups offline;
- Update and patch systems promptly;
- Test your incident response plan;
- Check your security team’s work; and
- Segment your networks.

“Business executives should immediately convene their leadership teams to discuss the ransomware threat and review corporate security posture and business continuity plans to ensure you can continue or quickly restore operations,” Neuberger wrote. She notes that ransomware attacks have affected organizations and hospitals around the world. As the federal government is working with other countries to hold ransomware actors and the countries that harbor them accountable, the private sector can assist by implementing these practices within their businesses. The White House also released a [fact sheet](#) and [guidance](#) to assist in carrying out these measures.

- Expanding the ability of covered entities to disclose PHI to avert a threat to health or safety when a harm is “serious and reasonably foreseeable,” instead of the current stricter standard which requires a “serious and imminent” threat to health or safety;

- Eliminating the requirement to obtain an individual’s written acknowledgment of receipt of a direct treatment provider’s Notice of Privacy Practices (NPP); and
- Modifying the content requirements of the NPP to clarify for individuals their rights with respect to their PHI and how to exercise those rights.

**OCR Publishes Summer 2021 Cybersecurity Newsletter** – On July 14, 2021, the Department of Health & Human Services, Office for Civil Rights (OCR, the HIPAA enforcement agency) published its [Summer 2021 Cybersecurity Newsletter](#), titled *Controlling Access to ePHI: For Whose Eyes Only?* In part, this newsletter focuses on information contained in a recent report of security incidents and data breaches, specifically findings that indicate that 39% of data breaches in the healthcare industry were found to have been perpetrated by insiders (such as employees), not by outside threat actors. The remaining 61% of analyzed data breaches were perpetrated by external threat actors—hackers and other cybercriminals.

The OCR reinforces the importance of various controls to assist in HIPAA Security Rule compliance and overall security of data systems that house protected health information (PHI), including:

- Information Access Management – This includes the implementation of policies and procedures for authorizing access to electronic PHI within an organization. This may include how access to each information system containing electronic PHI is requested, authorized, and granted, who is responsible for granting access, and what is the criteria for granting access. This should include a consideration of “role-based” access—basing access rights on the parameters of each individual’s job functions.
- Access Controls – This includes the implementation of technical controls to ensure only authorized persons are allowed access to electronic systems that house electronic PHI. This includes assigning a unique username and/or number for identifying and tracking user identity, emergency access procedures for obtaining electronic PHI in an emergency, automatic logoff procedures, and encryption and decryption mechanisms.

In the newsletter, the OCR emphasized:

*The rise in data breaches due to hacking as well as threats to ePHI by malicious insiders highlights the importance of establishing and implementing appropriate policies and procedures regarding these Security Rule requirements. Ensuring that workforce members are only authorized to access the ePHI necessary and that technical controls are in place to restrict access to ePHI can help limit potential unauthorized access to ePHI for both threats.*

This is yet another reminder to healthcare providers and their business associates of the need to implement or update a comprehensive HIPAA compliance program, including ongoing training and monitoring, to protect against both internal and external threat actors.



## Right of Access Initiative in Full Swing in 2021 and Continues

– On November 30, 2021, the Department of Health & Human Services, Office for Civil Rights (OCR) [announced](#) five enforcement actions against healthcare providers as part of the OCR’s “right of access” initiative, bringing the total number of enforcement actions under the initiative to 25 since inception approximately two years ago. Under HIPAA, providers and health plans generally have 30 days in which to provide a patient with “access” to the patient’s health records—either “view” access or copies of the records. In the latest five enforcement actions, the OCR settlements with the providers included corrective action plans, monitoring for a period of time, and financial penalties ranging from \$10,000 to \$100,000. The OCR continues to take this initiative seriously, and we are likely to see more enforcement actions in 2022.

**Healthcare Breach Report: Who is Getting Breached?** – In its [2021 Healthcare Data Breach Report](#), Critical Insight reported that “[d]ata on cyberattacks from the first half of 2021 shows criminals are changing targets within the healthcare ecosystem, with breaches increasing for outpatient facilities and business associates. The data also shows some long-term trends continuing, with overall attacks on an upward trend.” The report highlights 2020 as “a year memorable for both COVID-19 and an explosion of ransomware attacks.”

Although the number of breaches reported to the U.S. Department of Health & Human Services in the first half of 2021 declined from the second half of 2020, this number gives

“false hope,” since a breach like the [Blackbaud ransomware attack](#) was one of the biggest breaches of the year, impacting millions of individuals. Categories of breach incidents include theft, improper disposal, loss, unauthorized access/disclosure, and hacking/IT incident, the last of which “captures any breach that’s the result of criminal hackers or compromise in cybersecurity systems and is the main cause of breaches.”

Targets of cyberattacks are changing—outpatient family medicine and specialty clinics and business associates have become primary targets. The report also addresses the extreme costs associated with healthcare data breaches: according to IBM’s [Cost of a Data Breach Report 2021](#), an average of \$9.23 million, a 29.5% increase from IBM’s previous report.

The report includes suggestions for healthcare providers, including assessing third-party risk, management of business associate agreements, ransomware prevention and response, implementing strong access controls, and practicing basic security hygiene. Of course, these items are all important components of a compliant and active privacy and security program as required under HIPAA. Healthcare providers previously taking a casual approach to HIPAA compliance should take heed and consider updating, implementing, or supplementing their HIPAA compliance programs, including the educational component, to assist in preventing small and large-scale breach incidents and the collateral damage associated with such breaches.



Attorney Advertising: This publication is designed to provide Brach Eichler LLC clients and contacts with information they can use to more effectively manage their businesses. The contents of this publication are for informational purposes only. Neither this publication nor the lawyers who authored it are rendering legal or other professional advice or opinions on specific facts or matters. Brach Eichler LLC assumes no liability in connection with the use of this publication.

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

### Members

Isabelle Bibet-Kalinyak | 973.403.3131 | [ibibetkalinyak@bracheichler.com](mailto:ibibetkalinyak@bracheichler.com)

Riza I. Dagli | 973.403.3103 | [rdagli@bracheichler.com](mailto:rdagli@bracheichler.com)

Lani M. Dornfeld, HLU Editor | 973.403.3136 | [ldornfeld@bracheichler.com](mailto:ldornfeld@bracheichler.com)

John D. Fanburg, Chair | 973.403.3107 | [jfanburg@bracheichler.com](mailto:jfanburg@bracheichler.com)

Joseph M. Gorrell | 973.403.3112 | [jgorrell@bracheichler.com](mailto:jgorrell@bracheichler.com)

Carol Grelecki | 973.403.3140 | [cgrelecki@bracheichler.com](mailto:cgrelecki@bracheichler.com)

Keith J. Roberts | 973.364.5201 | [kroberts@bracheichler.com](mailto:kroberts@bracheichler.com)

### Counsel

Colleen Buontempo | 973.364.5210 | [cbuontempo@bracheichler.com](mailto:cbuontempo@bracheichler.com)

Shannon Carroll | 973.403.3126 | [scarroll@bracheichler.com](mailto:scarroll@bracheichler.com)

Ed Hilzenrath | 973.403.3114 | [ehilzenrath@bracheichler.com](mailto:ehilzenrath@bracheichler.com)

Debra W. Levine | 973.403.3142 | [dlevine@bracheichler.com](mailto:dlevine@bracheichler.com)

Caroline J. Patterson | 973.403.3141 | [cpatterson@bracheichler.com](mailto:cpatterson@bracheichler.com)

Jonathan J. Walzman | 973.403.3120 | [jwalzman@bracheichler.com](mailto:jwalzman@bracheichler.com)

Edward J. Yun | 973.364.5229 | [eyun@bracheichler.com](mailto:eyun@bracheichler.com)

### Associates

Lindsay P. Cambron | 973.364.5232 | [lcambron@bracheichler.com](mailto:lcambron@bracheichler.com)

Paul J. DeMartino, Jr. | 973.364.5228 | [pdemartino@bracheichler.com](mailto:pdemartino@bracheichler.com)

Susan E. Frankel | 973.364.5209 | [sfrankel@bracheichler.com](mailto:sfrankel@bracheichler.com)

Emily J. Harris | 973.364.5205 | [eharris@bracheichler.com](mailto:eharris@bracheichler.com)

James J. Ko | 973.403.3147 | [jko@bracheichler.com](mailto:jko@bracheichler.com)

Cynthia J. Liba | 973.403.3106 | [cliba@bracheichler.com](mailto:cliba@bracheichler.com)

Erika R. Marshall | 973.364.5236 | [emarshall@bracheichler.com](mailto:emarshall@bracheichler.com)

Roseland, NJ | New York, NY | West Palm Beach, FL | [www.bracheichler.com](http://www.bracheichler.com) | 973.228.5700

Stay Connected! Follow us on [LinkedIn](#), [Twitter](#), and [Facebook](#).