Report on
Medicare Compliance

Volume 32, Number 8 • February 27, 2023

Weekly News and Compliance Strategies on Federal Regulations, Enforcement Actions and Audits

Contents

HCCA

Managing Editor
Nina Youngstrom
nina.youngstrom@hcca-info.org

Copy Editor
Jack Hittinger
jack.hittinger@hcca-info.org

New Self-Disclosure Policy from U.S. Attorneys Has 'Significant Financial Incentives'

Voluntary self-disclosure (VSD) has taken a turn with a new policy from the nation's U.S. attorneys, who will now slash fines and forgo criminal charges when companies come forward with misconduct. But they may have to swallow criminal charges if the C-suite was involved, according to the first-ever United States Attorney's Offices' Voluntary Self-Disclosure Policy announced Feb. 22.[1]

The policy, which was developed by the Attorney General's Advisory Committee and approved by Deputy Attorney General Lisa Monaco, describes "the expectations of what constitutes" voluntary self-disclosures and their "clear and predictable benefits." The benefits include a penalty that's not more than 50% of the low end of the Sentencing Guidelines range for companies without aggravating factors. Companies with aggravating factors also are eligible for sharply reduced fines, but they're not off the hook from a criminal plea.

"This is at least an attempt by the Department of Justice to put its money where its mouth is and demonstrate its sincere desire to treat companies with an effective compliance program better than companies that are not investing in compliance the way that they should," said former federal prosecutor Anthony Burba, with Barnes & Thornburg LLP in Chicago.

continued on p. 7

BAAs Have 'Become Almost Noise,' But BAs Were Implicated in Almost Half of 2022 Breaches

When a hacker spoofed the email of an employee at a health care consulting firm, it set in motion a notification to clients that was mostly met with a shrug. The hacker had sent emails to the employee's clients with the intention of infiltrating their email accounts and gathering more contacts, but one of them recognized it was phishing and tipped off the consulting firm. Although the hacked email was shut down immediately, the consulting firm was concerned because some clients send unsecured protected health information (PHI) through email. As their business associate (BA), the consulting firm sent letters to clients who were potentially affected and explained the details of the security incident, said Regina Alexander, who worked for the consulting firm at the time. The response was surprising: about a third of the clients ignored the letter, another third asked one question about it and the rest were attorneys who wanted a meeting to discuss it, said Alexander, now a principal with BerryDunn.

The relative indifference was emblematic of the attitude toward business associate agreements (BAAs), Alexander said. "The key point is it's a document that has become almost noise. It's one of those check-the-box compliance items that people sign without reading," she explained. That's unfortunate because covered entities (CEs) pay the price when things go wrong with their BAs, Alexander said at a Feb. 9 webinar sponsored by the Health Care Compliance Association. Alexander noted that BAs were implicated in about 51% of the HHS Office for Civil Rights'

continued

(OCR) reportable breaches in 2022 affecting 500 or more people. More powerfully, about 89% of people affected by breaches last year were attributable to the cases involving BAs.

"It shows you where the risk is," she said. The CEs that landed on OCR's so-called wall of shame because of a BA include MCG Health, CommonSpirit Health, Texas Tech University Health Sciences Center and Shields Health Care Group Inc., all caused by hacking/IT incidents involving their network servers, according to OCR.

The HIPAA Privacy Rule allows covered entities to authorize a BA to use and disclose protected health information (PHI) "to carry out its legal responsibilities."[1] The BAA "must limit further disclosures of the protected health information for these purposes to those that are required by law and to those for which the business associate obtains reasonable assurances that the protected health information will be held confidentially and that it will be notified by the person to whom it discloses the protected health information of any breaches of confidentiality."

But some CEs aren't living up to that requirement, according to Alexander. "What's reasonable about two parties exchanging boilerplate agreements and not acknowledging on a deeper level what could be happening? A little more thought is necessary."

Report on Medicare Compliance (ISSN: 1094-3307) is published 45 times a year by the Health Care Compliance Association, 6462 City West Parkway, Eden Prairie, MN 55344. 888.580.8373, hcca-info.org.

Buck Stops With CE

On the surface it may not seem that way. HIPAA doesn't insist on oversight of BAs, said attorney Dena Castricone, with DMC Law LLC, who spoke at the webinar. It takes a hands-off approach, with OCR saying in an answer to a frequently asked question that "covered entities are not required to monitor or oversee the means by which their business associates carry out privacy safeguards or the extent to which the business associate abides by the privacy requirements of the contract."[2]

Castricone said CEs aren't required to do much before or after they engage the BA. "The only thing that HIPAA says is if the covered entity has actual knowledge of the business associate's material breach, the covered entity has to do something, but the actual knowledge standard encourages covered entities to take a head-in-the-sand approach," she said. Unless CEs do additional due diligence, the chances of a breach caused by the BA are higher, according to Alexander and Castricone.

"It is the covered entity that has the responsibility when something goes wrong," Castricone noted. "It's the covered entity's PHI." Although HIPAA requires BAs to notify the covered entity of a possible breach, it's the CE's job to report the breach to people and to HHS (and the media if more than 500 people are affected) unless the BAA requires the BA to report the breach.

Before CEs sign contracts with vendors, they should kick their tires, Castricone said. She encourages CEs to create due diligence forms and send them to vendors who will have significant access to PHI (see box, p. 4). Ask whether the potential BA has performed a security risk assessment as required by the HIPAA Security Rule and has a certification like HITRUST. "If you know your potential BA has achieved some of these things and has some baseline knowledge, that should give you a little comfort," she noted.

When it's time to execute the BAA, Alexander and Castricone suggest adding to OCR's model form.[3] "It's important to customize the BAA to meet your organization's needs," Castricone said. "It makes good business sense to use this document to provide as much protection to your organization as possible" (see box, p. 6).

For example, if CEs spell out in the contract with the BA that it must complete a security risk assessment and have policies and procedures about protecting electronic PHI but the BA drops the ball, "it's a material breach of your BAA and an opportunity to terminate it," Castricone said. Also, although HIPAA doesn't require cybersecurity insurance, CEs should require their BAs to have it for both the BA's and the CE's damages. "They normally address it in the master services agreement, but make sure you spell out in the business associate agreement and that in the event of a conflict, the BAA shall govern," she said.

BA Breach Reporting May Backfire

In their BAAs, CEs may shift breach reporting obligations to BAs, but that may not go as planned. For example, in Syracuse, New York, a medical group required its medical billing company to send breach notification letters to patients when it was responsible for a breach, Alexander said. But many patients who got the August 2022 letter thought it was a scam and tossed it in the garbage. Because of buzz about it in the community, a local news station reported on the letter to let the public know it was a legitimate breach notification. The incident probably brought more attention to the medical group than it would have generated by reporting the breach itself, defeating the purpose of shifting the breach reporting to the billing company, Alexander said. "It probably seems like a great thing for practices to minimize their exposure, but it backfired."

BAAs should also address encryption and multifactor authentication although they're not required by HIPAA, Castricone said. BAs would be required to encrypt the CE's PHI when they transmit it or it's at rest. If the BA bungles it and there's a ransomware attack, the CE would be able to extricate itself from the master services agreement, Castricone said. The same goes for multifactor authentication on any services or platforms where PHI is stored or transmitted.

Checklist for Reviewing Business Associate Agreements

Here's a template to help covered entities review their business associate agreements (BAAs). It was developed by Regina Alexander, a principal with BerryDunn. It also could be "reverse engineered for a business associate/vendor to review all the BAAs they have signed," she said (see story, p. 1). Contact Alexander at ralexander@berrydunn.com.

Business Associate (BA)/Vendor name		**Reviewer initials**	
Internal AP account # (if applicable)		**Date reviewed**	
Date of original contract/agreement		**Remediation pending? [Y/N]**	
Renewal/expiration date of original contract/ agreement		**Initial review status**	
Internal Business Lead/Department Overseeing Vendor/BA		**Final review status**	
Type of service provided by vendor/BA		**Risk level of vendor/BA**	
Review Step	**Response**	**Follow-up needed? [Y]**	**Additional notes/observations**
Business Associate Agreement (BAA) on-file? (Y/N)			
Format of BAA (hard copy, electronic)			
Is the BAA fully executed? (Y/N, if no, describe deficiency)			
If yes to BAA, date executed by CE & Name of Designee			
If yes to BAA, date executed by BA & Name of Designee			
Do the parties executing the BAA still represent the organizations? (Y/N)			
Is the contact information for notifications accurate for both parties? (Y/N)			
What is the time frame for the BA to notify the CE of a security incident or breach of PHI?			
What is the method of notification? (U.S. mail, fax, hand delivery, overnight, etc.)			
Is the BAA boilerplate (HHS OCR Sample Template, no special provisions)? (Y/N)			
If the BAA contains special/custom terms, do the terms include indemnification for losses? If yes, how much?			
If the BAA contains special/custom terms, do the terms include cyberinsurance? If yes, how much?			
Other custom terms?			
Are there terms in the Master Services Agreement or contract that potentially conflict with the BAA? (Y/N)			
If yes to conflicting terms, provide examples.			

"Don't leave it to your business associate to determine what reasonable safeguards are. It's your data," she said. "The covered entity is responsible for breach notification so it should dictate how the BA will protect the data."

Because of the risks posed by BAs, Alexander recommends that CEs perform retrospective audits of their BAAs (see box, p. 3). CEs should focus on high-risk relationships, such as vendors who provide release of information, chronic care management and utilization management, because they have access to the CE's electronic health records, and billing vendors, which have access to Social Security numbers and other patient data on claim forms.

Identify the vendors by getting a list from the accounts payable department and winnowing it from there. Some obviously don't have access to PHI (e.g., cleaning companies, website designers). Then determine whether you have a BAA that was signed by both parties. Was it before or after the HITECH Act? "You should have a HITECH-compliant BAA," Alexander said.

Contact Alexander at ralexander@berrydunn.com and Castricone at dena@dmclawllc.com. ✧

Endnotes

1. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000), https://bit.ly/3KwZR55.
2. U.S. Department of Health & Human Services, Office for Civil Rights, "Is a covered entity liable for, or required to monitor, the actions of its business associates?" FAQ, last reviewed January 9, 2023, http://bit.ly/3EvMX3v.
3. U.S. Department of Health & Human Services, Office for Civil Rights, "Model Business Associate Agreement," last accessed February 23, 2023, https://bit.ly/3lYtTEy.

Hospital Pays $21.6M in FCA Settlement; 'Worthless' Services Alleged

A long-term care hospital in Houston, Texas, has agreed to pay $21.6 million to settle false claims allegations that it improperly billed Medicare for services provided by unauthorized students and for services that were not performed or were "worthless," the U.S. Attorney's Office for the Southern District of Texas said Feb. 22.[1]

Cornerstone Healthcare Group Holding Inc. and CHG Hospital Medical Center LLC, doing business as Cornerstone Hospital Medical Center, provided extended medical and rehabilitative care to patients with multiple acute and/or chronic conditions. The hospital is not operating anymore as a long-term care hospital and CHG has been acquired by ScionHealth.[2]

According to the settlement, between Jan. 1, 2012, and December 2018, the government alleged that Cornerstone Hospital Medical Center billed Medicare for services provided by the "unauthorized and unlicensed students" of physicians Jorge Guerrero, Joel Joselevitz and Joseph Varon as if the services were performed by the patients' treating physicians.[3] The hospital also allegedly submitted claims to Medicare for services "not rendered while the alleged treating physicians were on foreign travel." And the government alleged the hospital billed Medicare for services that weren't supported by the patients' diagnoses or medical records "and for services that were either not rendered or so inadequate that they were worthless." Because the false claims allegedly were submitted knowingly to Medicare,

Due Diligence in Advance

Here are questions for covered entities to ask before entering into business associate agreements. They were provided by Dena Castricone, an attorney with DMC Law LLC. She noted the materials provided here are for educational purposes only and not as legal advice. Contact Castricone at dena@dmclawllc.com.

Initial Considerations Re: Business Associates

1. Will the vendor have access to protected health information (PHI) in any form to do work for you? If so, the vendor is a business associate (BA).
2. Be sure that you understand exactly what BA access entails (e.g., access to your systems, access to paper records, etc.). Analyze that access to determine whether it is necessary for the BA to carry out its functions for you. Limit access wherever reasonably possible.

Business Associate Due Diligence Questions

1. Has vendor previously signed a BAA with other customers?
2. Does vendor have HIPAA Security and Breach Notification Policies and Procedures that meet regulatory requirements under HIPAA? Please provide a copy of such policies or a table of contents of such policies that provide sufficient detail of the contents.
3. When did vendor last perform an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (i.e., a HIPAA security risk analysis that complies with 45 C.F.R.§ 164.308(a))?
4. How frequently does vendor perform such an analysis?
5. Has vendor implemented a security awareness and training program for all workforce members? If so, please describe the program.
6. Does vendor hold any certifications or other designations that evidence an understanding of and compliance with industry-recognized cybersecurity standards? If so, please describe each and provide proof of certification/designation (e.g., HITRUST, ISO 27001, SOC 2, etc.).

Cornerstone allegedly violated the False Claims Act (FCA), according to the settlement.

Cornerstone didn't admit liability and an attorney representing it in the case declined to comment.

The case was set in motion by a whistleblower, Natasha Lyons, who worked at Cornerstone Hospital Medical Center as a monitor tech and unit secretary. The Department of Justice intervened in the FCA lawsuit on Jan. 12, 2023, for purposes of settlement.

The complaint paints a picture of unnecessary care, including allegedly unnecessary bronchoscopies, medication errors and unnecessary lab tests. One of the physicians allegedly performed multiple bronchoscopies on Medicare patients regardless of medical necessity, up to the max that Medicare would cover. "In 2017, [the physician] performed over ten bronchoscopies on a single Medicare patient," according to the complaint.[4]

The whistleblower also alleged the hospital routinely billed Medicare for services, including cardiac telemetry, that weren't provided. Cardiac telemetry alerts staff when a patient's heart stops or indicates another kind of serious issue.

"Cornerstone Hospital often failed to connect patients to cardiac telemetry equipment," the complaint alleged. Even when it was performed, hospital staff didn't always print readouts to put in a patient's chart.

Paging Dr. Heart

When the whistleblower started working at Cornerstone Hospital Medical Center in April 2017, she said it didn't take long to notice the alleged fraudulent practices. For one thing, as a monitor tech, her job was to observe heart monitors through telemetry. The whistleblower said her supervisor had told employees to use the coded message "Call Dr. Heart" on the hospital communication system if they realized that a patient was not hooked up to telemetry. Almost every day, the call for Dr. Heart went out, but "no action was taken to connect the patients to telemetry," the complaint alleged. The whistleblower let two supervisors know but nothing changed.

The whistleblower also expressed concerns about fraudulent documentation to two managers but allegedly got no traction. In March 2018, the whistleblower was terminated.

Cornerstone allegedly billed Medicare for unnecessary laboratory tests, with patients sometimes getting the same kind of lab tests three or four times. "This occurred because each doctor who saw the patient ordered the same battery of tests. Defendants facilitated frequent unnecessary laboratory tests by installing Peripherally-Inserted Central Catheter ('PICC') lines in patients, which allowed blood to be easily drawn from a patient at any time," the complaint alleged.

Some Students Didn't Graduate From High School

The complaint describes the alleged use of the unauthorized and unlicensed students. The three physicians allegedly recruited students from Mexico and other foreign countries, but they weren't medical students, residents or some other kind of licensed medical professional. Some hadn't graduated from high school. Guerrero, Joselevitz and Varon allegedly allowed their students "to assist with surgeries, perform procedures and examine patients—alone and without in-person supervision by a licensed physician," according to the complaint.

Cornerstone hid the allegedly fraudulent practices from CMS and state inspectors, the complaint alleged. For example, during CMS inspections in November and December 2017, patient charts were hidden in the

CMS Transmittals and *Federal Register* Regulations, February 17-February 23

Transmittals

Pub. 100-04, Medicare Claims Processing

- National Coverage Determination (NCD) 50.3 - Cochlear Implantation Manual Update, Trans. 11,875 (Feb. 23, 2023)
- July 2023 Healthcare Common Procedure Coding System (HCPCS) Quarterly Update Reminder, Trans. 11,871 (Feb. 23, 2023)

Pub. 100-03, Medicare National Coverage Determinations

- National Coverage Determination (NCD) 50.3 - Cochlear Implantation Manual Update, Trans. 11,875 (Feb. 23, 2023)

Pub. 100-20, One-Time Notification

- Extensions of Certain Temporary Changes to the Low-Volume Hospital Payment Adjustment and the Medicare Dependent Hospital (MDH) Program under the Inpatient Prospective Payment System (IPPS) Provided by the Further Continuing Appropriations and Extensions Act, 2023, and the Consolidated Appropriations Act, 2023, Trans. 11,878 (Feb. 23, 2023)

Pub. 100-09, Medicare Contractor Beneficiary and Provider Communications

- The Supplemental Security Income (SSI)/Medicare Beneficiary Data for Fiscal Year (FY) 2021 for Inpatient Prospective Payment System (IPPS) Hospitals, Inpatient Rehabilitation Facilities (IRFs), and Long Term Care Hospitals (LTCHs), Trans. 11,870 (Feb. 23, 2023)

Pub. 100-05, Medicare Secondary Payer

- Significant Updates to Internet Only Manual (IOM) Publication (Pub.) 100-05 Medicare Secondary Payer (MSP) Manual, Chapter 3, Trans. 11,874 (Feb. 23, 2023)

Federal Register

Extension of timeline

- Medicare Secondary Payer and Certain Civil Money Penalties; Extension of Timeline for Publication of Final Rule, 88 Fed. Reg. 10,868 (Feb. 22, 2023)

medication room, under the whistleblower's desk or behind her computer. "Cornerstone Hospital concealed these charts because they revealed medication errors and Cornerstone Hospital's failure to follow patient care plans—namely, that procedures were scheduled but never performed," the complaint alleged.

On the day of one inspection, Cornerstone employees allegedly stashed a dead patient's body in a procedure room and put his chart under the whistleblower's desk because his family had not yet made arrangements to pick up the body or have him sent to a funeral home, according to the complaint. ✧

Endnotes

1. U.S. Department of Justice, U.S. Attorney's Office for the Southern District of Texas, "Medical Center pays over $21M to settle alleged false claims," news release, February 22, 2023, http://bit.ly/3xNhSEz.

Sample Provisions for Business Associate Agreements: More Than the Boilerplate

These are examples of BAA provisions that may provide more protection to covered entities. They were provided by Dena Castricone, an attorney with DMC Law LLC. She noted the materials provided here are for educational purposes only and not as legal advice. Contact Castricone at dena@dmclawllc.com.

Sample Provisions – Risk Analysis

3.2 Without limiting Business Associate's obligations under the HIPAA Rules, Business Associate agrees to perform a risk analysis to assess potential risks and vulnerabilities in its possession and develop, implement and maintain administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of any electronic PHI that is created, received, maintained or transmitted by Business Associate under this Agreement. **[Dena's note: This explicitly includes what the Business Associate is already obligated to do under the HIPAA Security Rule. Spelling it out here has a couple of advantages: (1) you can sue for breach of contract if the Business Associate doesn't do it; and (2) it is a clear reason for termination under 9.2 below.]** These measures shall be documented and be kept current, and must include, at a minimum, those measures that fulfill the requirements outlined in the HIPAA Rules, including compliance with the applicable requirements of the Security Regulations. Business Associate agrees to provide proof of compliance with section to Covered Entity upon request. **[Dena's note: Requiring proof is key.]**

Sample Provisions – Breach-Related

4.4 Reimbursement of expenses. Business Associate will reimburse Covered Entity for expenses reasonably incurred by Covered Entity in responding to a possible breach by Business Associate of Covered Entity's PHI, including, but not limited to, costs of investigation of the breach, compliance with the notification requirements set forth at 45 C.F.R. § 164.404 and responding to investigations by federal or state government authorities. Reasonable expenses include, but are not limited to, reasonable attorney's fees, publication expenses, logistics vendor expenses, establishment and maintenance of toll-free numbers, credit monitoring services, fines and penalties levied by any federal or state authority having jurisdiction and the value of Covered Entity staff time dedicated to the matter. **[Dena's Note: Breaches are expensive. A Business Associate's sole obligation under HIPAA is to notify the Covered Entity. Everything else falls to the Covered Entity.]**

4.5 At the option of Covered Entity, Business Associate shall make any notifications required under 45 C.F.R. §164.404 using notification language and a notification process approved by Covered Entity. If Covered Entity elects to make such notification, Business Associate agrees to reimburse Covered Entity for the costs outlined in section 4.4 above. **[Dena's Note: Under HIPAA, only the Covered Entity has the obligation to report to HHS and notify individuals. Business Associates only need to notify the Covered Entity. This clause contractually obligates the Business Associate to handle those items at the Covered Entity's direction.]**

Sample Provisions – Termination

9.2 Termination for cause. If Covered Entity determines that the Business Associate has materially breached the HIPAA regulations or this agreement, Covered Entity may either:

(a) Provide an opportunity to cure the breach, or (b) immediately terminate the agreement.

Notwithstanding anything to the contrary in this agreement, the services agreement or any other agreement between Covered Entity and Business Associate, if Covered Entity terminates this agreement for cause, Covered Entity may immediately terminate any services agreement that involves Business Associate's use of PHI without penalty. **[Dena's Note: This allows the Covered Entity to terminate the underlying agreement, which can sometimes be problematic. In a perfect world, when negotiating the underlying agreement, you should add a clause that says, "to the extent there is any conflict between this agreement and the Business Associate Agreement, the Business Associate Agreement shall govern."]**

Sample Provisions – Encryption and Multifactor Authentication (MFA)

3.3 Encryption. As a reasonable safeguard, Business Associate shall encrypt the Covered Entity's electronic PHI to render the PHI unusable, unreadable, or indecipherable to unauthorized individuals. To that end, Business Associate shall not transmit PHI electronically (including but not limited to transmission via email or text message) unless the PHI is encrypted during such transmission and further, shall ensure that all PHI stored electronically is encrypted. **[Dena's Note: This requires encryption across the board. Use this provision with Business Associates who will store or maintain large amounts of PHI.]**

3.4 Multifactor authentication. As a reasonable safeguard, Business Associate shall ensure that all electronic systems on which the Covered Entity's PHI resides uses a commercially reasonable form of MFA to ensure that only authorized individuals access such systems. **[Dena's Note: Not specifically required under HIPM but it is a reasonable safeguard. Failure to do this gives the Covered Entity the option to terminate.]**

2. Cision PR Newswire, "ScionHealth Completes Acquisition of Cornerstone Healthcare Group," news release, January 23, 2023, https://prn.to/3xOHMrz.
3. Settlement agreement, United States v. Cornerstone Group Holding and CHG Medical Center, http://bit.ly/3IuHo6q.
4. Complaint, United States v. Cornerstone Group Holding and CHG Medical Center, http://bit.ly/3ZhRHlf.

U.S. Attorneys Announce Self-Disclosure Policy

continued from page 1

The policy came down one month after the criminal division at the Department of Justice (DOJ) announced a corporate enforcement policy spelling out the rewards for companies that self-disclose their involvement in possible criminal wrongdoing.[2] The corporate enforcement policy, which was added to the Justice Manual, has similar benefits, but the U.S. attorneys' policy "is a little bit of a bigger deal than the one from the criminal division because it's national" and at least intended to be equally applied by all 94 U.S. attorneys' offices, Burba said. "This one is straightforward. The big carrot is to resolve your criminal liability without a criminal disposition if you fully disclose and meet other criteria with no aggravating factors." Even with aggravating factors, companies are eligible for a 50% to 75% penalty reduction. But things potentially could go awry, Burba said. "For a national policy like this where each U.S. attorney's office is its own small fiefdom, where one U.S. attorney gives 75% consistently and another gives 50%, will you end up in a forum shopping situation or will it be simple enough where it can be effectively and evenly applied across the U.S. attorney's offices?"

Companies Must Check Certain Boxes

According to the policy, each U.S. attorney will decide on a case-by-case basis whether a company's self-disclosure qualifies as a voluntary self-disclosure. It must meet these criteria:

1. Voluntary: "A disclosure will not be deemed a VSD under this policy where there is a preexisting obligation to disclose, such as pursuant to regulation, contract, or a prior Department resolution (e.g., non-prosecution agreement or deferred prosecution agreement)."
2. Timing: A disclosure must be made before an "imminent threat of disclosure or government investigation," before the conduct becomes publicly known, and "within a reasonably prompt time" after the company finds out about the misconduct.
3. Substance of the disclosure and accompanying actions: The disclosure is required to contain all relevant facts about the misconduct that the company knows about at the time of the disclosure. Although the U.S. attorney's office understands the company may not know "all relevant facts" when it discloses, the company should provide a "fulsome disclosure" of what it knows at the time and explain that it's based on a "preliminary investigation or assessment of information."

Cooperation and Remediation Are Required

If all boxes are checked, the U.S. attorney won't pursue a guilty plea, assuming the company also fully cooperates, appropriately remediates the criminal conduct and has no aggravating factors. The penalty will be no greater than 50% of the low end of the U.S. Sentencing Guidelines fine range.

It's another story if there are aggravating factors, which include misconduct that "1. poses a grave threat to national security, public health, or the environment; 2. is deeply pervasive throughout the company; or 3. involved current executive management of the company," according to the policy. Even if the company voluntarily self-disclosed, fully cooperated and remediated the criminal conduct, a criminal plea may be warranted. But there's still a payoff: the U.S. attorney will recommend to a sentencing court a 50% to 75% penalty reduction off the low end of the U.S. Sentencing Guidelines fine range or the penalty reduction in the alternate voluntary self-disclosure policy that's specific to the misconduct. And the company will be spared an independent monitor if it shows it has an effective compliance program. In terms of how that's defined, the U.S. attorney's office will consider DOJ resources, including *Evaluation of Corporate Compliance Programs*.[3]

The marginal differences in penalties between companies with and without aggravating factors is curious. "You could almost read it to suggest that you get a better deal" with aggravating factors, Burba said. Although only companies with aggravating factors are at risk of a criminal plea, "there are scenarios where they will get greater than a 75% reduction" in their penalties.

The voluntary self-disclosure policy is a response to the Sept. 15, 2022, Monaco memo, which directed every DOJ component "without a formal, written policy to incentivize" self-disclosure to "draft and publicly share such a policy."[4] The memo also reiterated that "corporations can best deter misconduct if they make clear that all individuals who engage in or contribute to criminal misconduct will be held personally accountable. In assessing a compliance program, prosecutors should consider whether the corporation's compensation agreements, arrangements, and packages (the 'compensation systems') incorporate elements—such as compensation clawback provisions—that enable penalties to be levied against current or former employees, executives, or directors whose direct or supervisory actions or omissions contributed to criminal conduct."

The policy's reduction in penalties are "significant," said former federal prosecutor Robert Trusiak, a lawyer in Buffalo, New York. They may provide leverage for clawing back compensation from executives as mentioned in the Monaco memo, which Trusiak has viewed with skepticism. "The basis for my skepticism was simply the power an executive wields within an organization," he explained. "The significant financial incentives associated with fine reduction really makes it genuine that companies with a self-disclosure will actually claw back executive compensation for those executives implicated in wrongdoing based on a simple cost-benefit analysis."

The self-disclosure policy was announced by the chair of the Attorney General's Advisory Committee, Damian Williams, U.S. attorney for the Southern District of New York, and Breon Peace, U.S. Attorney for the Eastern District of New York.

"DOJ is making a very clear statement they want companies to be in a position to work with integrity, hold themselves accountable and create an accountability culture in the company," Burba said. It's a message that has been hammered home by earlier documents, including the Federal Sentencing Guidelines and HHS Office of Inspector General's *Measuring Compliance Effectiveness: A Resource Guide*.

Contact Burba at tony.burba@btlaw.com and Trusiak at robert@trusiaklaw.com. ✧

Endnotes

1. U.S. Department of Justice, "United States Attorneys' Offices Voluntary Self-Disclosure Policy," memorandum, February 22, 2023, https://bit.ly/3It2amT.
2. U.S. Department of Justice, "Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy," updated January 2023, https://bit.ly/3ZQDs8e.
3. U.S. Department of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs*, updated January 2020, https://bit.ly/2Z2Dp8R.
4. U.S. Department of Justice, Office of Deputy Attorney General Lisa O. Monaco, "Further Revisions to Corporate Criminal Enforcement Policies Following Discussions with Corporate Crime Advisory Group," memorandum, September 15, 2022, https://bit.ly/3BqcDfk.

NEWS BRIEFS

◆ **Kandel & Associates P.A., a Baltimore-based law firm, and Nelson R. Kandel Esq., have settled allegations they failed to reimburse the government for certain Medicare payments the government made to medical providers on behalf of firm clients, the U.S. Attorney's Office for the District of Maryland said Feb. 23.**[1] The investigation stemmed from Medicare as Secondary Payer (MSP) provisions under the Social Security Act. "When an injured person receives a tort settlement or judgment, Medicare law requires persons or entities who receive the settlement or judgment proceeds, including the injured person's attorney, to repay Medicare for its conditional payments," the U.S. attorney's office said. "The Government alleges that, over many years, Medicare made conditional payments to healthcare providers to satisfy medical bills for firm clients. During that period, the firm negotiated for and received settlement proceeds for the firm's clients, but neither the firm nor its clients repaid Medicare for conditional payments it made to medical providers. This settlement resolves the Government's claims that the firm and Mr. Kandel failed to resolve at least twelve MSP debts." The law firm and Kandel agreed to pay $39,828.66 to resolve the MSP claims. They didn't admit liability in the settlement.

◆ **The HHS Office for Civil Rights (OCR) on Feb. 17 delivered two reports to Congress for 2021,** on HIPAA Privacy, Security, and Breach Notification Rule Compliance[2] and Breaches of Unsecured Protected Health Information.[3] In the first report, OCR said it "completed 573 compliance reviews and required subject entities to take corrective action or pay a civil money penalty in 83% (475) of these investigations. Two compliance reviews were resolved with RA/CAPs and monetary payments totaling $5,125,000. In the remaining 98 (17%) completed compliance reviews, OCR provided the covered entity or business associate with post-investigation technical assistance (3%), found insufficient evidence of a violation of the HIPAA Rules (11%), or lacked jurisdiction to investigate the allegations (3%). OCR issued one subpoena, and no audits were initiated." In the second report, OCR said it "initiated investigations into all 609 breaches affecting 500 or more individuals, as well as 22 breaches involving fewer than 500 individuals. OCR completed 554 breach investigations, through the provision of technical assistance; achieving voluntary compliance through corrective action; resolution agreements and corrective action plans; or after determining no violation occurred. Specifically, OCR resolved two breach investigations with resolution agreements, corrective action plans, and monetary payments totaling $5,125,000."

Endnotes

1. U.S. Department of Justice, U.S. Attorney's Office for the District of Maryland, "Maryland Law Firm Kandel & Associates, P.A., Agrees to Pay the United States Nearly $40,000 to Settle Claims That It Did Not Reimburse Medicare for Payments Made on Behalf of Firm Clients," news release, February 23, 2023, http://bit.ly/3YX4VUQ.
2. U.S. Department of Health & Human Services, Office for Civil Rights, *Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance For Calendar Year 2021*, February 17, 2023, https://bit.ly/3IQE6Ma.
3. U.S. Department of Health & Human Services, Office for Civil Rights, *Annual Report to Congress on Breaches of Unsecured Protected Health Information For Calendar Year 2021*, February 17, 2023, https://bit.ly/3SrPMs4.