International Journal of Innovation Scientific Research and Review
Vol. 05, Issue, 08, pp.5044-5054, August 2023
Available online at http://www.journalijisr.com
SJIF Impact Factor 2023: 6.599

ISSN: 2582-6131

Research Article

THE SENTENCING GUIDELINES, THE COVID-19 PANDEMIC, AND HEALTHCARE FRAUD

***Donald L. Buresh, Ph.D., Esq.**

Morgan State University.

Received 29th June 2023; Accepted 30th July 2023; Published online 30th August 2023

ABSTRACT

The article begins by examining the compliance components of the United States Sentencing Commission Guidelines 2021 as well as the benefits of fostering an ethical corporate culture through employing a carrot-and-stick approach. The Covid-19 Pandemic is briefly discussed, where both physicians and patients are considered to be potential perpetrators, along with the effect of the pandemic on the workforce. Self-disclosure issues are described, where the steps to be taken to minimize a False Claims Act (FCA) violation are highlighted. Finally, the Stark Law (SL) and Anti-Kickback Statute (AKS) are examined.

Keywords: Anti-Kickback Statute, Covid-19 Pandemic, False Claims Act, Healthcare Fraud, Overbilling, Patient Fraud, Physician Fraud, Stark Law.

INTRODUCTION

The article begins by examining the compliance components of the United States Sentencing Commission Guidelines 2021 (Guidelines) as well as the benefits of fostering an ethical corporate culture through employing a carrot-and-stick approach.The Covid-19 Pandemic is briefly discussed, where both physicians and patients are considered to be potential perpetrators, along with the effect of the pandemic on the workforce. Self-disclosure issues are described, where the steps to be taken to minimize a False Claims Act (FCA) violation are highlighted. Finally, the Stark Law (SL) and Anti-Kickback Statute (AKS) are examined.

COMPLIANCE COMPONENTS IN THE SENTENCING GUIDELINES

In this section, the compliance components of the Guidelines are discussed. The section defines the seven basic compliance components, and outlines the compliance components and small business. Because the Guidelines use a "carrot and stick" approach to help organizations self-regulate, the research inquires whether the Guidelines are effective. Finally, the paper asks whether the carrots inherent in the compliance components are sufficient to promote good corporate citizenship. Each topic is discussed in turn.

Definition of the Seven Basic Compliance Components

According to theGuidelines, for a compliance program to be effective, an organization must be diligent in detecting criminal conduct and promote a corporate culture that fosters ethical behavior and compliance to the law.[1] In pursuit of a compliance culture, it was recommended that an entity shall:[2]

1) Establish standards and procedures to prevent and detect criminal conduct;
2) Ensure that the organization possesses an effective compliance program, where the program has reasonable oversight and is periodically evaluated for safeguarding its effectiveness;
3) Employ reasonable efforts to include all company members, including individuals that may have engaged in illegal activities or conduct inconsistent with the compliance program.
4) Use reasonable steps to communicate with all employees and contractors about the compliance program and conduct effective training programs;
5) Warrant that the compliance and ethics program is followed, periodically evaluate its effectiveness, and provide an anonymous and confidential mechanism where employees can report or seek guidance on potential or actual criminal conduct;
6) Promote and enforce consistently throughout the organization via incentives and disciplinary measures to prevent or detect criminal conduct; and
7) Take reasonable steps to respond appropriately to criminal conduct and prevent future criminal conduct by periodically assessing the risk of criminal conduct.

The Guidelines noted that if the compliance program fails to detect a particular offense, it does not mean that the program was not generally ineffective in detecting and preventing criminal conduct.[3]Additionally, if the company is publicly traded, it must comply with the Sarbanes-Oxley Act of 2002.[4] If the organization is a federal government contractor or subcontractor, the organization must adhere to the Federal Acquisition Regulation (FAR).[5] Other compliance requirements apply to other industries. The good news is that these various regulations tend to complement each other.

Seven Basic Compliance Components and Small Business

The size of an organization is an issue when evaluating how a small business will abide by the seven basic compliance components listed above. The number of employees or the amount of annual revenue is

[1]*United States Sentencing Commission Guidelines Manual 2021*, UNITED STATES SENTENCING COMMISSION (2021), *available at*https://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2021/GLMFull.pdf.
[2]*Id.*
[3]*Id.*
[4]Steven D. Gordon, *Implementation of Effective Compliance and Ethics Programs and the FederalSentencing Guidelines*, CORPORATE COMPLIANCE ANSWER BOOK 2018 (2018), *available at*https://legacy.pli.edu/product_files/Titles/2470/%23205998_02_Corporate_Compliance_Answer_Book_2018_P3_20170915151415.pdf.
[5]*Id.*

a good indicator of an entity's size. For example, a company with 25 or fewer employees or annual revenue of less than $10 million may not have the resources to hire a full-time employee to ensure that the organization behaves ethically. However, when the number of employees in a firm is relatively small, individual employees tend to police themselves, ensuring compliance and good ethical behavior.[6]
As a firm expands and grows, resources become more plentiful. The company gains not only more revenue and profit but also more employees. In essence, the organization is experiencing increasing, but more likely, constant returns to scale.[7] When an organization earns, say, $50 million of annual revenue and approximately 100 or more employees, it probably has the resources to hire at least a compliance consultant or ensure that employee addresses compliance and ethical concerns on a part-time or full-time basis.[8] Furthermore, as an entity grows, the interaction between employees can become more formal, where individuals know less about the activities of others.[9] This lack of knowledge and interaction can breed potential criminal misconduct because of the anonymity in the workforce, where individuals may feel that they can behave unethically without being discovered.

Ethical behavior and compliance with law start with senior management.[10] In an organization of any size, it is essential to remember that compliance and ethics are not the same.[11] According to the Ethics and Compliance Initiative (ECI), ethics is the "study of right and wrong conduct"[12] or "the decisions, choices, and actions (behaviors) we make that reflect and enact our values."[13] In contrast, compliance is "[c]onforming or adapting one's actions to another's wishes, to a rule or to necessity. A compliance code would be intended to meet all legal requirements."[14] For example, suppose a child is thinking of stealing a candy bar. Does the child not steal the candy bar because they know that they will be punished for the action (compliance), or does the child not steal the candy bar because they know it is wrong to do so (ethics)? The best answer is that the child is ethical and does not steal the candy bar, whereas the second-best answer is that the child does not steal the candy bar for fear of retribution. Either way, the child does not steal the candy bar. The best answer is a subjective deterrent because it involves an internal restraint, while the second-best answer is an objective deterrent because it comprises an external restraint.

The following are significant benefits of fostering an ethical corporate culture:[15]

- **Boosts morale** – Employees want to work for an employer and fellow employees that they can trust who are honorable and honest;
- **Misconduct declines** – When creating a code of conduct that lists expectations of fair treatment and ethical behavior, firms are providing standards that employees can use to behave professionally;
- **Increases productivity** – Research demonstrates that maintaining ethical practices enhances better performance, particularly when the code of conduct aligns with the personal values of company employees; and
- **Improves compliance** – Although an action might be legal, it may not always be ethical, implying that ethics underpin compliance.

The benefits of generating an ethical corporate culture can be had by any organization, regardless of size.As a practical matter, the actions that an organization can take to encourage business ethics and nurture a culture of compliance include:[16]

- **Put corporate expectations in writing** – This may be difficult for tiny businesses but becomes increasingly important as the firm grows in stature. Even so, employees need an official, track able policy with teeth.
- **Have a dedicated compliance officer** – This may also be challenging for tiny businesses but becomes progressively vital as an entity expands. A Corporate Compliance Officer (CCO) with real poser should be appointed when appropriate. A CCO may be Corporate Counsel.
- **Hold employees accountable** – Accountability is essential in establishing a company's mission, values, and goals so that a culture of compliance is explicit and expressed for full-time, part-time employees, and contractors. This can be accomplished regardless of the size of an organization.
- **Communicate clearly and consistently** – Convey the corporate ethical policies and procedures clearly and consistently, ensuring that employees understand and appreciate how the violation of these policies and procedures will affect their jobs. This can also be attained regardless of the size of a firm.
- **Implement ethics training** – Ethical training is essential to ensure that employees understand what is expected of them and the consequences of violating ethical policies and practices. Formal training may be difficult for tiny businesses, typically employing informal training methods.

Even if some of the activities listed above may be difficult to achieve for a tiny business, a formal process is helpful if possible. For tiny businesses, it is essential to hire ethical employees so that the business can rely on the ethical and moral training an individual received from their family, religious upbringing, previous training, or surrounding circumstances.

Primary Carrots to Achieve Robust Compliance Programs

According to Brown Jackson and Cooper Grilli, the Guidelines employ a "carrot and stick" philosophy to incentivize corporations to self-police themselves regarding compliance and ethics to promote corporate responsibility.[17] The approach emerged because the United

[6] *Seegenerally*Laura J. Spence, *Does Size Matter? The State of the Art in Small Business Ethics*, 8 BUSINESS ETHICS, THE ENVIRONMENT&RESPONSIBILITY 3, 163-74 (Dec. 16, 2002), *available at*https://doi.org/10.1111/1467-8608.00144.
[7] STEVEN A. GREENLAW, & TIMOTHY TAYLOR, PRINCIPLES OF ECONOMICS 169 (OpenStax 2017), *available at*https://openstax.org/details/books/principles-economics-2e.
[8] Seegenerally, Tom Ewer, *Ethics and a Successful Small Business: Can You Have Both?*,HIVEAGE (n.d.), *available at*https://www.hiveage.com/blog/ethics-and-successful-small-business/#.
[9] *Id.*
[10] PowerDMS Staff, *Role of Ethics and Compliance in Corporate Culture*, POWERDMS (Dec. 29, 2020), *available at*https://www.powerdms.com/policy-learning-center/role-of-ethics-and-compliance-in-corporate-culture.
[11] *Id.*
[12] Ethics, *Glossary of Ethics and Compliance Terms*, ETHICS AND COMPLIANCE INITIATIVE (n.d.), *available at*https://www.ethics.org/resources/free-toolkit/toolkit-glossary/.
[13] *Id.*
[14] *Id*
[15] PowerDMS Staff, *supra*, note 10.
[16] *Id.*
[17] Ketanji Brown Jackson, & Kathleen Cooper Grilli, "*Carrot and Stick" Philosophy: The History of the OrganizationalSentencing Guidelines and the Emergence of Effective Compliance and Ethics Programs* 1.25, UNITED STATES SENTENCING COMMISSION (n.d.), *available at*https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2014/org_article.pdf.

States Sentencing Commission (Commission) recognized that: "1) vicarious liability means not all corporate defendants are alike; 2) responsible corporate actions can foster crime control; and 3) sentencing guidelines are rules that can incentivize good conduct."[18] Furthermore, the Commission's objectives for constructing the Guidelines were to define a model for good corporate citizenship and then employ the model to ensure that corporate sentencing was fair, where incentives existed for companies to control criminal actions.[19]
The question immediately comes to mind is whether the Commission's social engineering is effective. The first conspicuous issue is whether the "carrot" is mightier than the "stick."[20] The fines in the Guidelines are predicated on "(a) the pecuniary gain to the defendant, (b) the pecuniary loss to victims, or (c) an amount from a fine table, scaled to reflect the seriousness of the offense, which table goes up to a maximum of $165,000,000."[21] The maximum multiplier is three, so the maximum fine for the most severe offenses is $495 million (= 3 * $165 million).[22] The guidelines could require even higher fines if the financial loss can be easily calculated.[23]

However, this "stick" may be illusory because the associated Commission "carrot" may belittle it. Under §8C1.2(e), although the multiplier may be at most three, if mitigating factors exists, the multiplier can fall to at least 0.15.[24] For example, suppose that the base fine is $100 million. The actual fine could be at most $300 million (=3 * $100 million) or at least $15 million (= 0.15 * $100 million). The maximum fine will likely be 20 times the minimum at any given fine base level.[25] An issue with the Guidelines is that mitigating factors may increase the variation of fines rather than reduce the variation.The second issue with the Commission employing incentives is that ends and means can be confused. The Guidelines attempt to encourage organizations to harden internal mechanisms for deterring, detecting, and reporting criminal conduct by corporate agents and employees by specifying stringent penalties when entities fail to act ethically.[26] The sentencing structure in the Guidelines seeks to reward compliance plans, internal monitoring, and senior management's lack of criminal involvement. These are the means to the end of reducing corporate crime. They are not ends in themselves.[27]

Although the factors appear transparent, the cost of achieving a general deterrent is unclear. The unknown variables are:"(1) the degree to which compliance plans and internal monitoring reduce criminal activity, (2) the ability of courts to distinguish legitimate, effective internal monitoring from cosmetic or half-hearted attempts, and (3) the impact on general deterrence of reducing fines to a nominal level if such structural controls and procedures are institutionalized."[28] A better solution might be to assign mitigation credits on a provisional basis via a suspended sentence so that if additional criminal behavior occurs during the probationary period, the organization forfeits the mitigation credits attained under probation.[29]

[18] *Id.* at 1.61.
[19] *Id.*
[20] John C. Coffee Jr., *"Carrot and Stick" Sentencing:StructuringIncentives for OrganizationalDefendants*, 3 FED. SENT'G REP. 126 (1990), *available at* https://scholarship.law.columbia.edu/faculty_scholarship/528.
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Id.*

Are the Carrots Sufficient to Encourage Good Corporate Citizenship?

This empirical question can only be answered by statistical data analysis regarding corporate fines due to the Guidelines. Also, in performing the statistical analysis, probably a regression data analysis or, more likely, an analysis of variance, sufficiency criteria must be established before the analysis is conducted. One of the problems with such a statistical undertaking is that there would likely be no data on companies that are not repeat offenders that come to the attention of federal prosecutors. It is possible that managers or employees commit criminal acts yet are either not caught or not brought to the federal government's attention because the matter is handled privately. Thus, sufficiency is not a straightforward question to answer. Instead, it demands a detailed understanding of specific circumstances.

COVID-19 PANDEMIC AND THE WORK FORCE

This section addresses variety of topics concerning the Covid-19 and the work force. The section is divided into two subsections. There are the policy changes that occurred during the pandemic, followed by the work force issues. The first subsection deals with HIPAA flexibility for telehealth technology, the temporary changes in Medicare and Medicaid policies, telehealth licensing requirements, the prescribing of controlled substances, the Consolidated Appropriations Act (CAA) and the American Rescue Plan Act (ARPA), and the telehealth policy changes after the public health emergency. The second subsection speaks to work force issues, including the issues around working from home.

Policy Changes During the Covid-19 Pandemic

During the Covid-19 pandemic, the federal government took steps temporarily to provide and receive healthcare via telehealth.[30]The Health Resources Services Administration (HRSA) defined telehealth as the "use of electronic information and telecommunications technologies to support long-distance clinical health care, patient and professional health-related education, public health and health administration."[31] The technologies in telehealth include video-conferencing, the Internet, store-and-forward imaging, streaming media, and terrestrial and wireless communications.[32]

The six changes to healthcare administration via the Health Insurance Portability and Accountability Act (HIPAA) that have occurred due to the Covid-19 pandemic include:[33]

- HIPAA flexibility for telehealth technology;
- Temporary changes in Medicare and Medicaid policies;
- Telehealth licensing requirements and interstate compacts;
- Prescribing controlled substances;
- Consolidated the Appropriations Act and the American Rescue Plan Act regarding telehealth; and
- Telehealth policy changes after the Covid-19 public health emergency.

[30] *Policy Changes During Covid-19*, TELEHEALTH.HHS.GOV (n.d.), *available at*https://telehealth.hhs.gov/providers/policy-changes-during-the-covid-19-public-health-emergency/.
[31] *WhatisTelehealth? How Is TelehealthDifferent from TeleMedicine?*,HEALTHIT.GOV (n.d.), *available at*https://www.healthit.gov/faq/what-telehealth-how-telehealth-different-telemedicine.
[32] *Id.*
[33] *Policy Changes During Covid-19*, *supra*, note 1.

HIPAA Flexibility for Telehealth Technology

Due to the Covid-19 pandemic, health care providers now possess more flexibility to employ everyday technology. Covered health care providers under HIPAA may temporarily employ popular communication applications as long as the application is non-public facing.[34] A public-facing application is an application that is accessible from both an internal network and the Internet.[35] Examples of public-facing applications not allowed for temporary use under HIPAA are Facebook Live and Twitch.[36] Examples of video chat applications that are non-public facing are:[37]

- Apple FaceTime;
- Facebook Messenger video chat;
- Google Hangouts video;
- Zoom; and
- Skype,

while text-based applications that are non-public facing include:

- Signal;
- Jabber;
- Facebook Messenger;
- Google Hangouts;
- WhatsApp; and
- iMessage.

According to the Department of Health and Human Services (DHHS), health care providers that desire additional privacy protections should use technology vendors that are HIPAA compliant.[38] The vendors listed below claim to be HIPAA-compliant and are willing to enter into HIPAA business associate agreements:[39]

- Skype for Business / Microsoft Teams;
- Updox;
- VSee;
- Zoom for Healthcare;
- Doxy.me;
- Google G Suite Hangouts Meet;
- Cisco Webex Meetings / Webex Teams;
- Amazon Chime;
- GoToMeeting; and
- Spruce Health Care Messenger.

The Department of Health and Human Services Office for Civil Rights (DHHS-OCR) claimed that it did not review the business associate agreements offered by these vendors, and the presence on the list was not an endorsement. The DHHS-OCR did not endorse any of the video chat applications provided above.[40]

Temporary Changes in Medicare and Medicaid Policies

According to the DHHS, federal Covid-19 waivers and regulatory changes make it easier to deliver Medicare and Medicaid services to patients.[41] These temporary changes include:[42]

- **Patient location** – Health care providers may offer reimbursable telehealth services to patients located in their homes and outside of specific rural areas;
- **Practicing across state lines** – Health care providers may furnish telehealth and other services using communications technology when a patient is located across state lines subject to state-level policies and interstate agreements;
- **Relationship between patient and provider** – Health care providers may see new and existing patients using communications technology for telehealth and other types of visits;
- **Types of telehealth services covered** – The Center for Medicare and Medicaid Services (CMS) has dramatically expanded the list of services that can be provided by telehealth and over the telephone during the pandemic;
- **Types of eligible providers** – In general, a health care eligible to bill Medicare is eligible to bill for telehealth during the pandemic; and
- **Supervision of health care providers** – Health care providers may supervise their services through audio and video communications and in-person.

Telehealth Licensing Requirements and Interstate Compacts

Depending on state and federal policies, health care providers can temporarily deliver telehealth across state lines.[43]Various interstate compacts address whether the following health care providers can give services across state lines:[44]

- **For Physicians** – Interstate Medical Licensure Compact (IMLC);
- **For Nurses** – Nurse Licensure Compact (NLC);
- **For Psychologists** – Psychology Interjurisdictional Compact (PSYPACT);
- **For Physical Therapists** – Physical Therapists Compact (PTC);
- **For Emergency Medical Services Workers** – Emergency Medical Services Compact (EMSC); and
- **For Speech Language Therapists** – Audiology and Speech-Language Pathology Interstate Compact (ASLP-IC).

Prescribing Controlled Substances

During the Covid-19 pandemic, authorized health care providers may prescribe controlled substances by telehealth without an in-person medical examination.[45] The Drug Enforcement Administration (DEA)

[34] *Policy Changes During Covid-19: HIPAA Flexibility for Telehealth Technology,* TELEHEALTH.HHS.GOV (n.d.), *available at*https://telehealth.hhs.gov/providers/policy-changes-during-the-covid-19-public-health-emergency/hipaa-flexibility-for-telehealth-technology/.
[35] Esther Christopher, *Detecting Intrusions on Public-Facing Applications and Machines*, MANAGEENGINE.COM (Mar. 7, 2021), *available at*https://www.manageengine.com/log-management/cyber-security/detecting-intrusions-on-public-facing-applications-and-machines.html#:~:text=The%20term%20%22public%20facing%22%20refers,from%20the%20Internet%20as%20well.
[36] *Policy Changes During Covid-19 : HIPAA Flexibility for Telehealth Technology*, *supra*, note 5.
[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] *Id.*

[41] *Policy Changes During Covid-19:Temporary Changes in Medicare and Medicaid Policies,* TELEHEALTH.HHS.GOV (n.d.), *available at*https://telehealth.hhs.gov/providers/policy-changes-during-the-covid-19-public-health-emergency/medicare-and-medicaid-policies/.
[42] *Id.*
[43] *Policy Changes During Covid-19:TelehealthLicensingRequirements and Interstate Compacts,* TELEHEALTH.HHS.GOV (n.d.), *available at*https://telehealth.hhs.gov/providers/policy-changes-during-the-covid-19-public-health-emergency/telehealth-licensing-requirements-and-interstate-compacts/.
[44] *Id.*

[45] *Policy Changes During Covid-19:PrescribingControlled Substances*, TELEHEALTH.HHS.GOV (n.d.), *available*

has made two temporary modifications regarding the prescription of controlled substances during the pandemic. First, a practitioner may prescribe a controlled substance employing telemedicine when a patient is not in a hospital or clinic registered with the DEA.[46] Telemedicine is the "exchange of medical information from one location to another using electronic communication, which improves patient health status."[47] Telemedicine involves various applications and services, including wireless tools, email, two-way video, Smartphone's, and other methods of telecommunications technology.[48] Second, a qualifying practitioner may prescribe buprenorphine to new and existing patients with an opioid use disorder, where a patient is evaluated by telephone.[49]

Consolidated the Appropriations Act and the American Rescue Plan Act Regarding Telehealth

TheConsolidated the Appropriations Act (CAA)and the American Rescue Plan Act (ARPA) expanded telehealth funding and reimbursement during the Covid-19 pandemic.[50] Under the CAA, Rural Emergency Hospitals (REHs) became eligible Medicare originating sites for telehealth, permitting patients to be located at an REH when receiving telehealth services. However, the REH must be classified by the HRSA as an originating rural site to bill Medicare.[51] Also, under the CAA, patients may temporarily receive telehealth services in their homes, such as counseling, psychotherapy, and psychiatric evaluations.[52] However, the patient must have had at least one in-person evaluation by the behavioral health care provider to be eligible for a telehealth visit.[53] Under the ARPA, Emergency Rural Development Grants (ERDG) for rural health care may be used to increase telehealth capabilities, including health care information systems and behavioral health services.[54]

Telehealth Policy Changes After the Covid-19 Public Health Emergency

The DHHS took various steps to expedite the adoption of telehealth during the pandemic.[55] Many changes will lapse at the end of the Covid-19 public health emergency, while some changes will be permanent.[56] According to the DHHS, the Covid-19 public health emergency will end on October 13, 2022.[57] The CAA has specified a 151-day extension period before the temporary policies expire, providing a transition period.[58] The permanent changes include:[59]

- Medicare patients may receive telehealth services, including audio-only services, in their home or any part of the country, provided certain conditions are satisfied; and
- The CY 2022 Telehealth Update Medicare Physician Fee Schedule (PDF) codified the continued coverage of video-based mental health visits for Federally Qualified Health Centers (FQHCs) and Rural Health Clinics (RHCs) permanently.

The changes that will be phased out are:[60]

- Increased flexibility regarding where a patient receives Medicare telehealth services, where the restrictions that were in place before the pandemic will control;
- Medicare reimbursement for mental health telehealth services will again require an in-person visit within six months of initial assessment and every twelve months after that;
- Medicare reimbursement for telehealth visits provided by physical therapists, occupational therapists, speech-language pathologists, and audiologists will no longer be permitted;
- Medicare will no longer cover audio-only visits for physical health examinations; and
- FQHCs and RHCs will not be reimbursed as distant site telehealth providers for non-mental health services.

One issue healthcare providers will likely experience are patients who are upset because they may believe that the temporary changes in health care are permanent.

WORK FORCE ISSUES

Given the various rule changes described above, health care providers are faced with learning how to employ telecommunications technology in performing their jobs. Most health care providers are comfortable interacting with patients in person. Health care providers face the challenge of providing the same or greater level of services using telehealth and telemedicine applications. Healthcare providers may find such activities challenging to do because they are unaccustomed to working with technology. In other words, health care providers seemingly face a steep learning curve when interacting with patients electronically.A second, and more insidious issue, is health care providers adjusting back to pre-pandemic behaviors after the end of the public health emergency. Health care providers may have become accustomed to the temporary changes and engage in pandemic behaviors in a post-pandemic world. This possibility is ripe for out-of-compliance issues to crop up, forcing health care providers to alter their behavior again.

Working from Home

According to Chow, there are ten challenges when working from home. The first five challenges deal with the following work-from-home issues experienced by employees:[61]

- Developing blurred work-life boundaries;
- Inadequate practical equipment;
- Hovering supervisors;
- Employee isolation; and

*at*https://telehealth.hhs.gov/providers/policy-changes-during-the-covid-19-public-health-emergency/prescribing-controlled-substances-via-telehealth/.

[46] *Id.*

[47] *TelemedicineDefinition*, EVISIT (n.d.), *available at*https://evisit.com/resources/telemedicine-definition/.

[48] *Id.*

[49] *Policy Changes During Covid-19:PrescribingControlled Substances*, *supra*, note 15.

[50] *Policy Changes During Covid-19:Consolidated the Appropriations Act (CAA) and the American Rescue Plan Act (ARPA) RegardingTelehealth*, TELEHEALTH.HHS.GOV (n.d.), *available at*https://telehealth.hhs.gov/providers/policy-changes-during-the-covid-19-public-health-emergency/consolidated-appropriations-and-american-rescue-plan-acts-2021/.

[51] *Id.*

[52] *Id.*

[53] *Id.*

[54] *Id.*

[55] *Policy Changes During Covid-19:Telehealth Policy Changes After the Covid-19 Public Health Emergency*, TELEHEALTH.HHS.GOV (n.d.), *available at*https://telehealth.hhs.gov/providers/policy-changes-during-the-covid-19-public-health-emergency/policy-changes-after-the-covid-19-public-health-emergency/.

[56] *Id.*

[57] *Id.*

[58] *Id.*

[59] *Id.*

[60] *Id.*

[61] James Chow, *10 Common Challenges of Working From Home &Their Solutions for Employers*, EVERHOUR BLOG (Aug. 22, 2022), *available at*https://everhour.com/blog/challenges-of-working-from-home/.

- Resolving technical challenges.

The second five challenges address the issues regarding remotely working for employers:[62]

- Increased cybersecurity risk;
- Mis-aligned team performance;
- Employee loyalty and retention;
- Remote hiring; and
- Providing emotional support.

Traditionally, a home is a space away from public life. Many individuals treat it as a sanctuary. Almost by definition, homes are not as secure as offices. Compliance may be more challenging to achieve because of the openness of homes.[63] Second, when working in an office, an employer usually owns the hardware and software an employee uses. At home, an employee may not have access to the same kind of equipment as in an office. Also, an employee's equipment may not be as secure as office equipment. This fact may make it harder to comply with corporate security policies and government laws.[64] When individuals work from home, there may be a lack of trust in an employee's work ethic. This may encourage employees to cut corners and not strictly comply with corporate policies and government laws.[65] Human beings are social animals, and apparent isolation may adversely affect employee performance. Employees that are unaccustomed to working alone may not be as thorough as they would be if they were working on site. If so, compliance may suffer.[66] Some synergies occur when people congregate together and work together. When employees are isolated from the Covid-19 pandemic, these synergies may not occur because of the lack of communication among employees. Again, compliance may suffer because employees may not know the breadth of rules that should be obeyed.[67]

With a distributed workforce, all data and communications are transacted in the digital space. Any cybersecurity incident can have financial and reputational consequences, mainly when compliance is paramount.[68] When employees work virtually, there is always the risk of misaligned performance, more than when employees work on-site. The use of virtual tools must be carefully monitored to ensure that compliance standards are met.[69] Many employees strive to advance within a company. When employees work remotely, they have less visibility, which may lead to cutting corners when it comes to compliance to ensure that a task is completed on time. In terms of compliance, this can be a dangerous scenario.[70] When employees work remotely, managers may not meet them face-to-face. Managers learn a great deal about new hires from visual cues. When hiring an employee remotely, these are absent, and potential violations of compliance principles may be ignored.[71] Finally, in an on-ground environment, employees emotionally support each other. Emotional support is likely lacking in a virtual environment. The lack of emotional support may encourage employees to evade compliance principles to gain recognition from their peers.[72]

[62] *Id.*
[63] *Id.*
[64] *Id.*
[65] *Id.*
[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] *Id.*

THE COVID-19 PANDEMIC AND HOW PHYSICIANS CONFRONTED IT

This section addresses the Covid-19 pandemic and how physicians confronted it. This section contains four subsections. The first subsection deals with the issues surrounding billing Medicare during the pandemic. The second subsection talks about monitoring for errors in billing. The next subsection highlights the reasons why physicians and hospital staff are mandated to take billing training. Finally, the last subsection examines what physician activities will promote an audit from the OIG. Each subsection is explained in turn.

Educational Front

Physicians should be aware that some doctors continue to bill Medicare and patients for the most expensive office visits.[73] The services that are provided must correspond to the conditions present, treated, and then documented and billed. Physicians must understand that medical doctors can be scrutinized by Medicare, where upcoding is fraud. In particular, Medicare considers a physician guilty based on the code billed, notably if the medical record does not support the code. Although regulations may be rolling back, this is not occurring regarding fraud. Data analysis is being adjusted to identify physicians whose practice patterns deviate from normal behavior.[74]

Inaccurate coding puts a physician at risk of losing their license to practice medicine.[75] Inaccurate coding also risks the financial well-being of the hospital where the five physicians work. The five physicians should compare their billing habits with the other physicians in the hospital who have the same specialty. Suppose there are no other physicians at the hospital with the same specialty as the five physicians in question. In that case, the billing activities of other hospitals should be examined to see if the five physicians are upcoding.[76] If the five physicians are outliers, they need to be trained regarding proper billing and the risks of upcoding. Suppose any one of the five physicians is upcoding and adamant regarding their right to code for their services as they please. In that case, the hospital should seriously consider terminating its contract with the physician.
There is also the risk of under-coding or not billing enough money for medical services rendered. Although under-coding can result in legitimate monies not being collected from Medicare or the patient, the risk of losing a physician's medical license is not at issue. One could argue that it is probably better to under-code than up-code because upcoding bears the risk of losing a medical license and having to pay back the additional money billed.[77]The Office of Inspector General (OIG) has warned physicians that doctors are responsible for billing Medicare at the appropriate levels for office visits.[78] For example, a New York anesthesiologist had to pay back approximately $2 million in 2017 for improper billing, where 16-minutes of face time did not occur. Also. The argument that a physician's patients are always sickest when they meet with a medical doctor should be supported by evidence. A 15-minute office visit demolishes this argument.[79]

Finally, an over-reliance on checkboxes for documentation may precipitate overbilling. Such behavior may result in physicians cutting

[73] Alex Tate, *Key Precautions to Consider to AvoidOverbilling*, PHYSICIAN'W WEEKLY (Feb. 26, 2018), *available at*https://www.physiciansweekly.com/key-precautions-to-consider-to-avoid-overbilling.
[74] *Id.*
[75] *Id.*
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *Id.*

and pasting medical notes rather than writing them down for each patient. Cutting and pasting medical notes is plagiarism and invites scrutiny. Saving a minute may not be worth the cost of a physician losing their medical license.[80] All these issues should be revealed to the five physicians in question.

Monitoring Front

Errors in billing can be innocent or intentional. In either case, it can result in legal action that may harm a physician or the establishment where the physician practices medicine. Steps to control billing errors include:[81]

- Ensure patient information is correct and aligned adequately with data;
- Avoid upcoding;
- Utilize the latest medical coding manual;
- Avoid duplicate billing;
- Verify insurance benefits and coverage in advance; and
- Hire a professional medical biller.

The basic idea is that proper billing is based on integrity. A physician should focus on the long-term goal of staying in business correctly billing patients and Medicare, not billing as much money as one can for services rendered. Essentially, physicians should not be penny-wise and dollar-foolish. Monitoring billing does not infringe on a physician's right to treat their patients as they see fit. Instead, it is a discovery mechanism to weed out medical doctors abusing their discretion in being paid. It is essential that monitoring billing be viewed in this light so that abuses in billing do not occur or are minimized.

Training Front

The services provided should correspond to the conditions present in a patient, treated, and then documented and billed. Physicians must understand that their billing practices can be scrutinized by payors such as Medicare, where upcoding may constitute fraud. Physicians should understand that Medicare considers a medical doctor guilty based on the code billed, mainly if the medical record does not support the code billed. If found guilty, a physician may lose their license to practice medicine.Inaccurate coding also impinges on the integrity of the hospital, including its financial well-being. The OIG has warned physicians that doctors are responsible for billing Medicare at the appropriate levels for office visits. The argument that a physician's patients are always sickest when they meet with a medical doctor should be supported by evidence. An over-reliance on checkboxes for documentation may precipitate overbilling. Such behavior may result in physicians cutting and pasting medical notes rather than writing them down for each patient. Cutting and pasting medical notes is plagiarism and invites scrutiny. Saving a minute may not be worth the cost of a physician losing their medical license.

For the reasons stated above, all physicians and staff at the hospital are mandated to take the billing training that the hospital will offer within the next two months. The training will be conducted online to accommodate physician schedules. Physicians that fail to take this training at the end of two months will be suspended from practicing medicine at the hospital until the training has been completed. This training is vital because complying with the principles and practices therein will prevent potentially unnecessary litigation from originating patients and payors such as Medicare.

Auditing Front

According to the OIG, various activities can trigger an audit. For example, an audit can be triggered when physicians or hospitals employ billing codes that reflect a more severe illness or a more expensive treatment than provided. Another example is using a higher evaluation and management (HEM) code for a new or existing patient than is necessary. A third example is the misuse of modifier 25 on claims. Modifier 25 permits extra payment for separate E/M services provided on the same day as a procedure. Upcoding can occur when modifier 25 is appended on claims that are not significant, not separately identifiable, or not above and beyond the care typically associated with the procedure. Auditing can also occur when a physician:

- Did not actually render services;
- Rendered unnecessary services;
- Improperly performs a service;
- Supervises an unqualified employee;
- Supervises an employee that has been excluded from federal health care programs; or
- Gave virtually worthless services.

The results of an audit can be substantial, where the monies paid back can be in the millions of dollars.

Thus, to reduce the likelihood of an audit by an external payor such as Medicare, the hospital will periodically conduct internal audits of physician billing practices on a semi-annual basis. The intent of these internal audits is not to interfere with physician billing practices but to ensure that patients are appropriately billed based on services that are rendered. The intent of an internal audit is to flag issues before external payors become aware of them, allowing the hospital to correct billing errors promptly to prevent unnecessary litigation.

COVID-19 PANDEMIC AND THE PERPETRATION OF FRAUD

This section illuminates how physicians and patients perpetuated healthcare fraud during the Covid-19 pandemic. The first subsection talks about physicians as perpetrators, while the second subsection is concerned with patients as perpetrators. The final subsection describes threshold issues relating to healthcare fraud for the OIG and other federal and state organizations.

The Physician as Perpetrator

According to Levine and Levine, LLP, the primary reason that healthcare providers commit fraud is for financial gain.[82] When a healthcare provider increases the number of tests, treatments, and other services, they can collect additional money from private and public insurance companies, such as Medicare or Medicaid.[83] Another reason healthcare providers may commit fraud is out of the goodness of their hearts, mainly when patients cannot afford out-of-pocket costs, whereby providers overbill to pay for necessary medical

[80] *Id.*

[81] Simon Hughes, *How to Avoid Common MedicalBilling and Coding Errors*, CORONIS HEALTH (Oct. 27, 2020), *available at*https://www.coronishealth.com/blog/how-to-avoid-medical-billing-and-coding-errors/.

[82] *Why Do Doctors Commit Healthcare Fraud?*,LEVINE & LEVINE, LLP (Dec. 4, 2021), available at https://www.levine-levine.com/blog/2021/december/why-do-doctors-commit-healthcare-fraud-/#:~:text=The%20main%20motivation%20that%20healthcare,the%20goodness%20of%20their%20hearts.

[83] *Id.*

treatments.[84] Although the intentions of the healthcare provider are reasonable, it is still fraud.

Various tactics have been employed to commit healthcare fraud that may be unknown to the patient, including:[85]

- **Double billing** – This happens when a physician submits multiple insurance claims for the same service;
- **Phantom billing** – This occurs when a physician bills for services that are never rendered;
- **Upcharging**– Physicians may bill for a more expensive service than the patient received.
- **Kickbacks** – This may occur between healthcare providers if one offers the other money or other benefits in exchange for patient referrals.
- **Giving unnecessary tests and treatment** – Healthcare providers may conduct unnecessary examinations or prescribe unnecessary treatments to make more money;
- **Waiving copays** – This happens when a doctor waives a patient's copay and bills the insurance company to make up the difference.

For a physician, the penalties can include up to five years in prison, hundreds of thousands of dollars in fines, probation, civil fines or restitution, or loss of a medical license.[86]

Patients as Perpetrators

Patients and other individuals can also commit healthcare fraud. For example, patients and other individuals can engage in:[87]

- **Bogus marketing** – Convince people to provide their health insurance identification number and other personal information to bill for non-rendered services, steal their identity, or enroll them in a fake benefit plan;
- **Identity theft/identity swapping** – Employing another individual's health insurance or allowing another individual to use their insurance; or
- **Impersonating a health care professional** – Offering or billing for health services or equipment without a license.

Fraud that involves prescriptions includes:[88]

- **Forgery** – Creating or using forged prescriptions;
- **Diversion** – Diverting legal prescriptions for illegal uses, such as selling your prescription medication; or
- **Doctor shopping** - Visiting multiple providers to get controlled substances or prescriptions from medical offices that engage in unethical practices.

One issue with this type of fraud is that the individuals committing the fraud may be poor people who do not earn sufficient income to survive and engage in these activities. This statement does not condone the activities of such individuals. Instead, the purpose of exposing this kind of fraud is to help understand why the fraud occurs in the first place.

Threshold Issues

One should never forget that the OIG and other federal and state entities are organizations with limited resources. They cannot pursue all reports of wrongdoing merely because they receive a tip from a whistleblower that theft is occurring. It must be worth it to the organization to pursue a perpetrator. In other words, the benefits of the investigation (including potential fines and criminal penalties) must exceed the costs of the investigation. It is preferred a benefit-cost ratio that is used when deciding whether to investigate a particular violation. This is a critical piece of information that could potentially alert potential wrongdoers how a federal or state agency or a private insurance company decides to pursue criminal or civil action. Presuming that the benefit-cost ratio is an unpublished statistic, it is likely unpublished because to publish the statistic would help perpetrators decide how much fraud they could commit before invoking an audit by the OIG or some other federal or state agency.

ISSUES REGARDING SELF-DISCLOSURE

This section is focused on issues regarding self-disclosure. This section possesses five subsections. The first subsection describes the Self-Referral Disclosure Protocol (SRDP) that was created by CMS to identify and resolve issues affecting federal healthcare programs. The next subsection addresses several other self-disclosure options. The third subsection talks about the liability associated with overbilling and the FCA. The fourth subsection describes the steps to be taken to minimize the effects of the FCA. In the final subsection, specific recommendations are listed to minimize the adverse effects of an OIG audit, including how to approach the OIG without waiving legal rights.

Options for Self-Disclosure

The CMS has created the SRDP to help identify and resolve issues that adversely affect federal healthcare programs that are defined in 42 U.S.C. 1320a-7b(f).[89] The SRDP is to all persons that may have received an overpayment due to an actual or potential violation of Section 1877 of the Affordable Care Act (ACA), and raises potential criminal or civil liabilities.[90] Disclosing parties should not disclose the same conduct under the SRDP and the Office of Inspector General self-disclosure protocol (OIG-SDP).[91]The required documents for complete disclosure include the SRDP Disclosure Form, the Physician Information Form, and the Financial Analysis Worksheet.[92] The initial disclosure and any additional supplemental submissions must possess a certification signed by the disclosing party or the Chief Executive Officer (CEO) of an entity, or another individual authorized by the organization to disclose the issue to the CMS.[93] The document must testify to the truthfulness of the information contained therein.[94] The disclosure must be submitted electronically to 1877SRDP@cms.hhs.gov and a hard copy of the disclose to the CMS. If the disclosing party files for bankruptcy, changes ownership or designated representative, the disclosing party must inform CMS within 30 days.[95] As soon as CMS receives the submission, CMS will institute a verification process that will review disclosing party

[84] *Id.*
[85] *Id.*
[86] *Id.*
[87] *Health Care Fraud*, FEDERAL BUREAU OF INVESTIGATION (n.d.), *available at*https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/health-care-fraud.
[88] *Id.*
[89] *Provider Self-disclosure Protocol* 63 FED. REG. 58,400 (Oct. 30, 1998), *available at*https://oig.hhs.gov/authorities/docs/selfdisclosure.pdf.
[90] *CMS Voluntary Self-referral Disclosure Protocol*, CENTERS FOR MEDICARE AND MEDICAID SERVICES (Jan. 2017), *available at*https://www.cms.gov/Medicare/Fraud-and-Abuse/PhysicianSelfReferral/Self_Referral_Disclosure_Protocol.
[91] *Id.*
[92] *Id.*
[93] *Id.*
[94] *Id.*
[95] *Id.*

financial statements, notes, disclosures, and other supporting documents that are not protected by attorney-client privilege.

CMS will not accept payments of possible overpayments until their investigation is completed. However, disclosing parties may deposit funds in an interest-bearing escrow account to show CMS that they have set aside monies to repay the amount owed.[96] The disclosing party should include a report of its internal investigation, recognizing that CMS is not bound by the findings of the disclosing party. The internal investigation should include the nature and extent of the improper or illegal practice, the discovery and response to the matter, as well as certifying the document. The investigative methodology may consist of all claimed affected by the disclosure or statistically representative sample of the claims affected by the matter.[97]

Other Options for Self-Disclosure

The OIG possesses several self-disclosure processes that can be employed to report possible fraud in the DHHS programs.[98] Health care providers, suppliers, and other individuals or entities that are subject to civil monetary penalties can employ the Provider Self-Disclosure Protocol (PSDP) to voluntarily disclose evidence of fraud that they discovered.[99] The advantage of self-discovery is that providers have the opportunity to avoid disruptions and additional costs affiliated with investigations directed by the federal government and civil or administrative litigation.[100] OIG contractors with a FAR-based contract may use the Contractor Self-Disclosure Program (CSDP) to disclose violations of the FCA, including criminal laws regarding fraud, conflict of interest, bribery, and gratuity.[101] Entities that are HHS grant recipients or sub-recipients are also required to disclose possible criminal violations of federal involving fraud, bribery, or gratuity violations that may affect the federal award. Furthermore, HHS award recipients must also voluntarily disclose conduct that creates liability under the Civil Monetary Penalty Law (CMPL), 42 U.S.C. § 1320a-7a, or any other conduct that might violate civil or administrative laws.[102] Disclosing parties (DP) should not disclose the same conduct under the SRDP and the OIG-SDP.[103]

The OIG expects a disclosing party to conduct an internal investigation and report its findings to OIG in its submission. Suppose a disclosing party cannot complete its internal investigation before it sends its submission to OIG. In that case, an entity must certify that it will finish its investigation 90 days from its initial submission.[104] The disclosure report must be submitted via the OIG's website at:

https://oig.hhs.gov/compliance/self-disclosure-info/provider-self-disclosure-protocol/

The submission should consist of identifying information about the health care provider, the owner or controller of the disclosing party; and the disclosing party's designated representative.[105]The disclosing party should also provide a concise statement of the conduct and transactions that give rise to the violation, a statement of what federal laws were potentially violated, and the federal health care programs affected by the disclosed conduct.[106] The disclosing party should also provide an estimate of the damages or that the estimate will be completed within 90 days after the initial submission.[107] If actual damages are known, the amount of actual damages should be submitted instead of the estimated damages.

The disclosing party should describe its corrective actions after discovering the offending conduct.[108] The disclosing party should also state whether a government agency or contractor is currently investigating the matter or any other matter. The government agency and its individual representatives should be identified.[109] The disclosing party must reveal the individual authorized to enter into a settlement agreement. The disclosing party must certify that to the best of the authorized representative's knowledge, the information in the disclosing party's disclosure is truthful and based on a good faith effort to bring the matter to the government's attention to resolve potential liability.[110]

Overbilling and False Claims Act Liability

The ACA established an SRDP to reduce disclosing party liability and the potential penalties owed. Section 6402 of the ACA created a deadline for reporting and returning overpayments by the later of sixty (60) days after the date in which the overpayment was identified; or the due date of any corresponding cost report.[111]Once the disclosing party submits an SRDP and receives a confirmation email from CMS, the DP's obligation under Section 6402 is suspended until a settlement is entered, the disclosing party withdraws the SRDP, or CMS removes a service provider from the SRDP.[112][113]

The OIG established the various SDPs to reduce disclosing party liability and the potential penalties owed. Section 1128J(d)(2) of the Social Security Act (SSA) demands that a Medicare or Medicaid overpayment must be reported and returned by (1) the date that is 60 days after the date on which the overpayment was identified or (2) the date any corresponding cost report is due, if applicable, whichever is later.[114] If an overpayment is retained beyond this deadline, a liability is created under the CMPL, section 1128A of the SSA, and the FCA, 31 U.S.C. 3729.[115]

Steps to Minimize the Effects of a False Claims Act Violation

Throughout the entire OIG investigation, the disclosing party should diligently act in good faith so that OIG need not employ compulsory compliance methods. A lack of cooperation by a disclosing party may adversely affect the resolution of the matter, including treble damages.[116] The factor that OIG uses to reduce the amount owed include:[117]

[96] *Id.*
[97] *Provider Self-disclosure Protocol*, *supra*, note 1 at 58,402.
[98] *Self-Disclosure Information*, DEPARTMENT OF HEALTH AND HUMAN SERVICES: OFFICE OF INSPECTOR GENERAL (n.d.), *available at*https://oig.hhs.gov/compliance/self-disclosure-info/.
[99] *Id.*
[100] *Id.*
[101] *Id.*
[102] *Id.*
[103] *Id.*
[104] *OIG'sHealth Care Fraud Self-Disclosure Protocol*, DEPARTMENT OF HEALTH AND HUMAN SERVICES: OFFICE OF INSPECTOR GENERAL (Apr. 17, 2013), *available at*https://oig.hhs.gov/documents/self-disclosure-info/1006/Self-Disclosure-Protocol-2021.pdf.
[105] *Id.*
[106] *Id.*
[107] *Id.*
[108] *Id.*
[109] *Id.*
[110] *Id.*
[111] *CMS Voluntary Self-referral Disclosure Protocol*, *supra*, note 2.
[112] *Id.*
[113] 42 C.F.R. § 401.305 (b)(2)(ii).
[114] *Id.*
[115] *Id.*.
[116] Stacy C. Gerber Ward, *To Disclose or Not To Disclose, That is the Question*, VON BRIESEN& ROPER, S.C. (Aug. 15, 2017), *available at*https://www.vonbriesen.com/legal-news/3592/to-disclose-or-not-to-disclose-that-is-the-question.
[117] *CMS Voluntary Self-referral Disclosure Protocol*, *supra*, note 2.

- The nature and extent of the improper or illegal practice;
- The timeliness of the self-disclosure; and
- The cooperation in providing additional information about the disclosure.

It should be remembered that OIG is not obligated to reduce the amount owed even when the disclosing party cooperates with the government agency. OIG will consider these factors when individually determining the amount owed by the disclosing party.[118]

Specific Recommendations

It is recommended that a disclosing party fully cooperate with an OIG investigation subject to the constraint that it does now waive its legal rights, particularly attorney-client privilege. Negotiations with OIG should be friendly and not adversarial, ensuring that OIG understands that the disclosing party wants the matter resolved in a timely manner, where it is conveyed to OIG that the disclosing party has taken reasonable steps to prevent future occurrences of improper or illegal activity.As for the fate of wrongdoers within the organization, including the Chief Financial Officer (CFO), it is recommended that the organization not fire these individuals until the government investigation is completed. If the wrongdoers decide to remain at the entity, they should be relieved of their duties so that no additional harm can be done. If the wrongdoers are terminated, they may not be able to help the firm during the investigation. It would be detrimental to the organization not to have their cooperation during the inquiry.

THE STARK LAW AND THE ANTI-KICKBACK STATUTE

This section consists of three subsections. In the first subsection, the SL is discussed along with potential liability under the law. The second subsection talks about AKS and possible liability under this law. In the final subsection, the paper describes various policies and procedures that serve as best practices to avoid improper referrals and remunerations, conceivably violation the SL, the AKS, or both.

Stark Law Liability

The SL, or the Physician Self-Referral Law (PSRL), refers to Section 1877 of the Social Security Act (SSA). Under SL, a physician is prohibited from referring a patient to an organization with which the physician, or an immediate family member, has a financial interest, ownership interest or compensation relationship for the furnishing of a designated health service (DHS) unless a specific exemption is satisfied.[119] A physician is defined by SL as doctor of medicine or osteopath medicine, dentist, podiatrist, optometrist, or chiropractor.[120] An immediate family member is a (1) husband or wife; (2) birth or adoptive parent, child, of sibling; (3) step-parent, stepchild, step-brother, or step-sister; (4) father-in-law, mother-in-law, son-in-law, daughter-in-law, brother-in-law, or sister-in-law; (5) grandparent or grandchild; spouse of grand-parent or grandchild.[121] A DHS consists of:[122]

- Clinical laboratory services;
- Occupational physical therapy;
- Out-patient speech therapy;
- Out-patient speech-language pathology services;
- Radiology and other imaging services;
- Radiation therapy services and supplies;
- Durable medical equipment and supplies;
- Parenteral and enteral nutrients, equipment, and supplies;
- Prosthetics, orthotics, and prosthetic devices and supplies;
- Home health services;
- Outpatient prescription drugs; and
- Inpatient and outpatient hospital services.

Based on the definitions above, a physician that works at a hospital must fully disclose in writing whether they or any member of their immediate family have a financial relationship with any company that engages the list of DHS activities above. If the physician that has such a financial relationship, a condition for continuing to work at the hospital is that the physician must divest themselves of that relationship. If a member of the physician's immediate family has a financial relationship with an organization that provides DHSs to the hospital, either the immediate family member must divest themselves of the relationship or the hospital must terminate its relationship with the physician. Because there is the possibility that an immediate family can purchase a financial interest in a DHS entity after a physician has responded negatively to the hospital's questionnaire, the physician should be required to provide the hospital with new information as circumstances change, or annually, whichever is sooner.

Anti-Kickback Statute Liability

The AKS prohibits any person (42 U.S.C. § 1320a-7b(b)) from knowingly and willingly paying, soliciting, offering, or receiving remuneration (anything of value) to induce or reward the referral or recommendation of federal health care program business.[123] Remuneration can consist of:[124]

- Goods or services provided for free or below fair market value (FMV);
- Payments for services that are not provided or not necessary;
- Provision of space or equipment for free or below FMV;
- Discounts or rebates;
- Gift cards and other cash equivalents;
- Meals, tickets, and entertainment;
- Business opportunities that are not commercially reasonable;
- Waivers of copayments or deductibles; or
- Opportunity to generate a profit.

An example of a federal health care program would be Medicare, Medicaid, TRICARE, the Children's Health Insurance Program, and veteran's programs. Medicare Parts C and D are included, but the Federal Employees Health Benefits Program is not included.Another example would be if a physician were to receive medical equipment for their practice at below FMV in exchange for a referral or recommendation of Medicare business. Still another example would be if a physician received office space for free in exchange for a referral or recommendation.

Policies and Procedures as Best Practices

Physicians and other hospital staff should be trained to avoid improper referrals and remuneration issues. The training should provide general principles and specific interactive examples on how to avoid SL and AKS liabilities. The training should probably take

[118] *Id.*
[119] 42 U.S.C. § 1395nn(a).
[120] *Id.*
[121] *Id.*
[122] 42 U.S.C. § 1395nn(h)(6).
[123] Kate Dunn, *Nuts and Bolts of the Anti-KickbackStatute and BeneficiaryInducements CMP*, ALBANY LAW SCHOOL (n.d.).
[124] *Id.*

about 60 to 90 minutes to complete. It is probably advisable to have separate SL and AKS training modules. For physicians, the training should probably be more in-depth than the training for other hospital staff, if only because physicians are directly liable under these laws. The training should likely be done semi-annually or annually.

CONCLUSION

As the article examined the compliance components of the Guidelines as well as the benefits of fostering an ethical corporate culture through employing a carrot-and-stick approach, it became apparent that the Guidelines were an excellent source of a compliance strategy. The Covid-19 Pandemic showed that physicians could be considered as potential perpetrators because they were the individuals were either diagnosing patients or receiving medical information from patients. Patients could also be thought of as potential perpetrators because they were the individuals giving medical information to physicians. Self-disclosure was shown to be paramount to ensure that physicians take steps to minimize FCA violations. Finally, SL and AKS were examined to further help physicians avoid breaking the law.

Donald L. Buresh Biography

Donald L. Buresh earned his Ph.D. in engineering and technology management from Northcentral University. His dissertation assessed customer satisfaction for both agile-driven and plan-driven software development projects. Dr. Buresh earned a J.D. from The John Marshall Law School in Chicago, Illinois, focusing on cyber law and intellectual property. He also earned an LL.M in intellectual property from the University of Illinois Chicago Law School (formerly, The John Marshall Law School), an LL.M. in cybersecurity and privacy from Albany Law School, graduating summa cum laude, and is currently earning an LL.M. in financial compliance and risk management from Albany Law School. Dr. Buresh received an M.P.S. in cybersecurity policy and an M.S. in cybersecurity, concentrating in cyber intelligence, both from Utica College. He has an M.B.A. from the University of Massachusetts Lowell, focusing on operations management, an M.A. in economics from Boston College, and a B.S. from the University of Illinois-Chicago, majoring in mathematics and philosophy. Dr. Buresh is a member of Delta Mu Delta, Sigma Iota Epsilon, Epsilon Pi Tau, Phi Delta Phi, Phi Alpha Delta, and Phi Theta Kappa. He has over 25 years of paid professional experience in Information Technology and has taught economics, project management, negotiation, managerial ethics, and cybersecurity at several universities. Dr. Buresh is an avid Chicago White Sox fan and keeps active by fencing épée and foil at a local fencing club. Dr. Buresh is a member of the Florida Bar.

List of Abbreviations

Abbreviation	Description
ACA	Affordable Care Act
AKS	Anti-Kickback Statute
ARPA	American Rescue Plan Act
ASLP-IC	Audiology and Speech Language Pathology Interstate Compact
CAA	Consolidated Appropriations Act
CCO	Corporate Compliance Officer
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CMS	Center for Medicare and Medicaid Services
Commission	United States Sentencing Commission
CSDP	Contractor Self-Disclosure Program
DEA	Drug Enforcement Administration
DHHS	Department of Health and Human Services
DHHS-OCR	Department of Health and Human Services Office for Civil Rights
DHS	Designated Health Service
ECI	Ethics and Compliance Initiative
EMSC	Emergency Medical Services Compact
ERDG	Emergency Rural Development Grants
FAR	Federal Acquisition Regulation
FCA	False Claims Act
FMV	Fair Market Value
FQHC	Federally Qualified Health Centers
Guidelines	United States Sentencing Commission Guidelines
HEM	Higher Evaluation and Management
HIPAA	Health Insurance Portability and Accountability Act
HRSA	Health Resources Services Administration
IMLC	Interstate Licensure Compact
NLC	Nurse Licensure Compact
OIG	Office of Inspector General
OIG-SDP	Office of Inspector General Self-Disclosure Protocol
PDF	Physician Fee Schedule
PSDP	Provider Self-Disclosure Protocol
PSRL	Physician Self-Referral Law
PSYPACT	Psychology Interjurisdictional Compact
PTC	Physical Therapists Compact
REH	Rural Emergency Hospitals
RHC	Rural Health Centers
SL	Stark Law
SOX	Sarbanes-Oxley Act
SRDP	Self-Referral Disclosure Protocol
SSA	Social Security Act

Miscellaneous Considerations

Author Contributions: The author has read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest.

Acknowledgments: Not applicable

****