hfma™

massachusetts-rhode island chapter

Virtual Roundtable:
Telehealth & Hot Topics in Compliance

Friday, April 9th from 10:00 – 11:30 am EST

www.MA-RI-HFMA.org

Introduction

COVID-19 has transformed the delivery of health care. Chief among the changes is the rise in the prevalence of telehealth. In this roundtable, we'll discuss the myriad issues posed by telehealth, including delivery platforms, the regulatory landscape, billing/reimbursement, privacy, and IT security. We'll also go around-the-horn and address the hot compliance topics of the moment. In this interactive session, you'll hear from health care leaders from hospitals, health plans, and law firms who will share perspectives and best-practices. Participants will have a chance to ask questions and participate in the discussion.

Learning Objectives:

Understand Telehealth billing/reimbursement, privacy, and IT security compliance considerations, as well as Telehealth as a delivery model.

Hear from industry and legal colleagues on the current compliance hot topics facing healthcare organizations, especially compliance professionals.

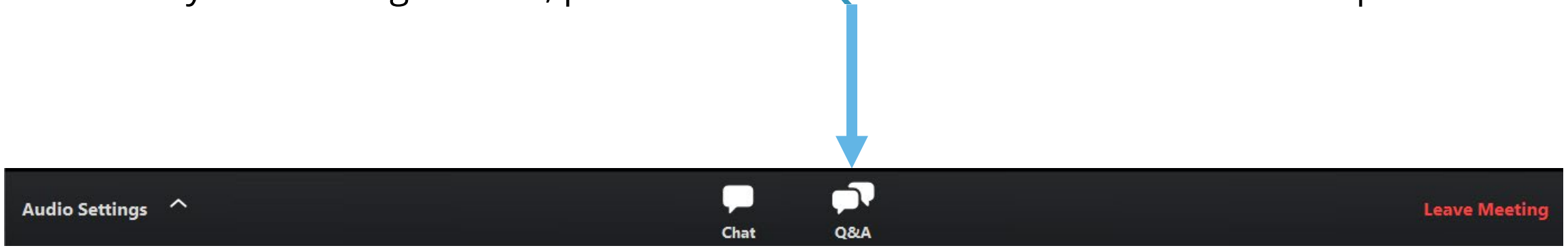
Learn best practices from the practical experiences of fellow industry colleagues

Earn CPE and CEU Credits

- Number of Credits: **HFMA 1.5 / CPE 1.8**
- Please note, in order to receive CPE Credits attendees must answer three polling questions as they are presented by the speakers

Zoom controls and functionality

- All attendees will be placed on mute for the entire length of the call
- At any time during this call, please **use the Q&A function in Zoom** to ask questions



Speakers

Rebecca Mishuris, MD

Chief Medical Information Officer

BMC

Kyle Faget

Partner

Foley & Ladner LLP

Dhara Satija

Senior Manager

Deloitte & Touche LLP

Donna Schneider

VP, Corporate Compliance and Internal Audit

Lifespan

Garrett Gillespie

VP, Deputy General Counsel & Corporate Compliance Officer

BMC

Larry Vernaglia

Partner

Foley & Ladner LLP

Polling Question #1

What industry sector do you represent?

A. Hospital
B. Physician practice
C. Post-acute
D. Integrated health system
E. Other

Polling Question #2

How many years have you been a healthcare compliance professional?

A. Less than 2 years
B. 3-5 years
C. 5-7 years
D. 7-9 years
E. 10+ years

Agenda

1. Telehealth – Recent Highlights *(Dr. Rebecca Mishuris and Kyle Faget)*
2. Compliance Hot Topics Post Covid-19 *(Larry Vernaglia, Donna Schneider, Garrett Gillespie)*
3. Open Q&A

The information in this presentation is current as of 4/9/2021

Telehealth – Recent Highlights

Rebecca Mishuris, MD

Kyle Faggot

Polling Question #3

How has your organization's telehealth utilization changed as a result of the COVID-19 pandemic?

A. Low utilization pre-pandemic, increase in utilization during the pandemic
B. High utilization pre-pandemic, continued high utilization during pandemic
C. Low utilization pre-pandemic, no change in utilization during pandemic

Telehealth – BMC Story

Rebecca Mishuris, MD

Telehealth – Q&A

Rebecca Mishuris, MD

Kyle Faggot

Polling Question #4

Will you be continuing to use telehealth as established delivery channel?

A. Yes
B. No
C. TBD

Compliance Hot Topics Post Covid-19

Donna Schneider

Garrett Gillespie

Larry Vernaglia

Polling Question #5

What issues keep you up at night worrying about your Compliance Plan? (You may select more than one option)

A. Billing & Coding / Provider Documentation
B. Risk adjustment
C. HIPAA and Privacy Risks (Data breaches, snooping in EMRs, sharing without consent)
D. The Cures Act implementation
E. The CARES Act requirements
F. Changes to Stark and Anti-Kickback
G. Interoperability

Polling Question #6

Have you planned on how to educate your organization regarding the January 2021 changes to Stark and the Anti-Kickback Statute? (Please note you can select more than one option, if you are selecting one of the "Yes" responses.)

A. No – I haven't even thought about it
B. No – I have no idea what to do
C. Yes to the Board/Committee with a presentation in conjunction with legal
D. Yes to the Board/Committee with a presentation by myself
E. Yes to the Board/Committee by hiring outside legal counsel to present
F. Yes to the Management team

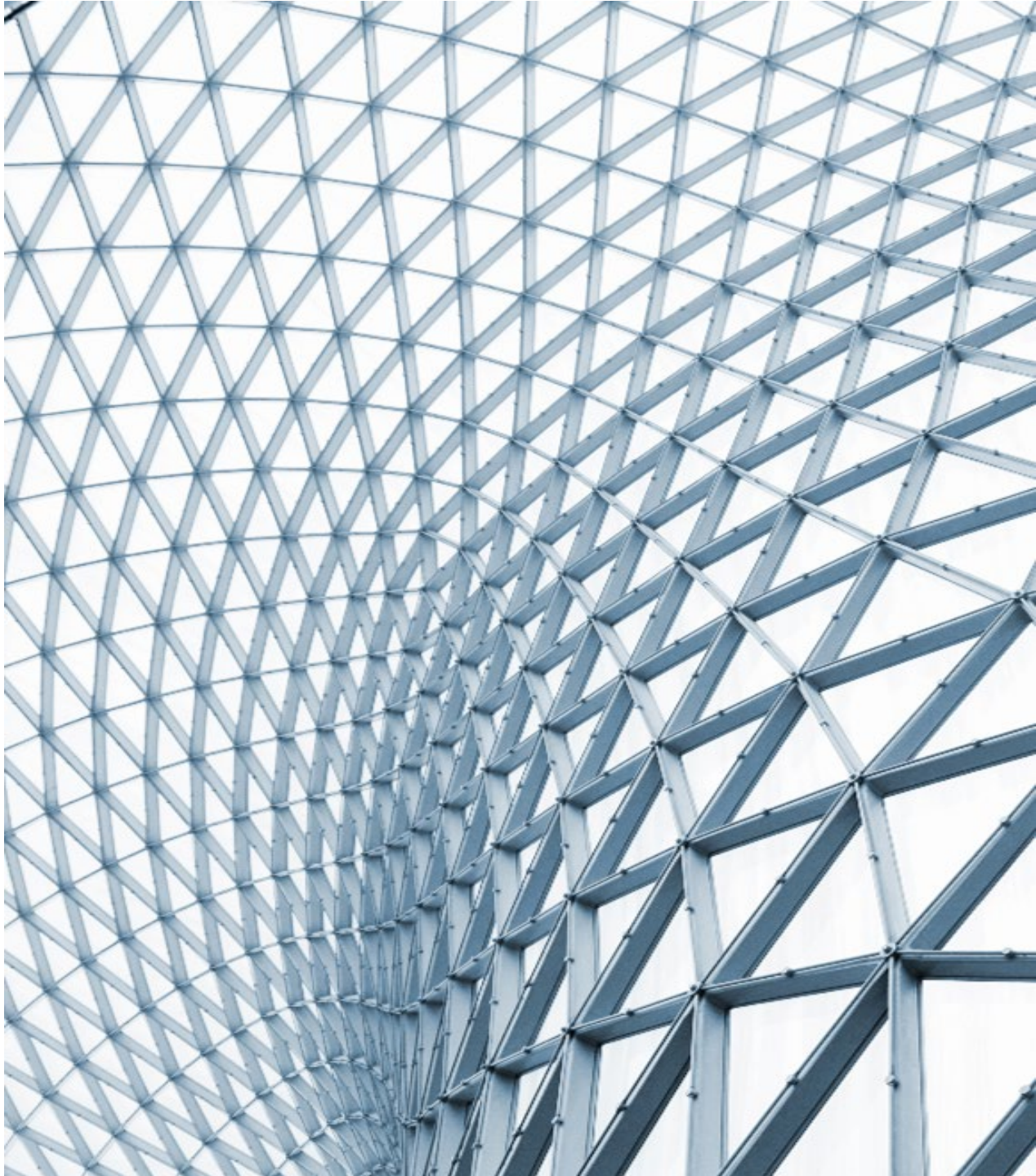
Polling Question #7

Are you aware of all the CMS waivers that your organization is leveraging today?

A. Yes
B. No
C. Somewhat

Open Q&A

Thank You!



Telehealth – Recent Highlights

Social and Economic Factors Are Enabling Virtual Health

The social and economic impacts of COVID-19 limit the ability for many individuals to obtain care; as such, there has been an emergence of virtual health as a primary channel of care thanks to regulatory leeway and shifting consumer expectations

UNPRECEDENTED CIRCUMSTANCES

COVID-19 brought forth a series of unprecedented events with the declaration of a global pandemic and widespread stay-at-home orders, driving further needs in our communities, especially amongst the most vulnerable

FINANCIAL PRESSURES

COVID-19 drove unemployment rates higher than ever recorded, as businesses shut down due to social distancing requirements, , putting increased financial strain on individuals

IMPACTS OF LONG-TERM DISTANCING

With stay-at-home orders impacting 330 million Americans daily, the risk of loneliness, isolation, and depression increase, posing short- and long- term health consequences

EMPHASIS ON SAFETY

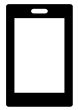
Long-term physical distancing and concern for exposure to COVID-19, particularly for the most vulnerable populations, has necessitated ways of receiving care outside traditional health care facilities

REGULATORY IMPACT

- CMS issued a blanket waiver and Interim Final Rule to increase patient access to virtual care during the COVID-19 Public Health Emergency (PHE)
- CMS increased reimbursement for 80 additional services, paying at the same rate as in-person visits when delivered via telehealth systems
- Department of HHS is waived potential penalties under federal HIPAA for telehealth services, during this emergency
- CMS outlined the Hospital Without Walls program in March and expanded it in November to provide eligible hospitals with regulatory flexibility to treat eligible patients in their homes
- Commercial payers have followed CMS' lead and begun to reimburse for virtual services

Virtual Health Adoption

Use of Technology to Delivery Health Care



A covered health care provider that wants to use audio or video communication technology to provide telehealth to patients during the COVID-19 nationwide public health emergency **can use any non-public facing remote communication** product that is available to communicate with patients.

→ Covered health care providers may use popular applications that allow for video chats**, including Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, Zoom, or Skype**, to provide telehealth without risk that OCR might seek to impose a penalty for noncompliance with the HIPAA Rules related to the good faith provision of telehealth during the COVID-19 nationwide public health emergency.

The Office for Civil Rights (OCR) at the Department of Health and Human Services (HHS) is exercising its enforcement discretion **to not impose penalties for noncompliance with the HIPAA Rules** in connection with the good faith provision of telehealth using such non-public facing audio or video communication products during the COVID-19 nationwide public health emergency.

→ Providers are **encouraged to notify patients that these third-party applications** potentially introduce privacy risks, and providers should enable all available encryption and privacy modes when using such applications.

This exercise of **discretion** applies to telehealth provided for any reason, regardless of whether the telehealth service is related to the diagnosis and treatment of health conditions related to COVID-19.

→ It is important to note that the use of; **Facebook Live, Twitch, TikTok, and similar video communication applications are public facing**, should **not** be used in the provision of telehealth by covered health care providers.

For example, a covered health care provider in the **exercise of their professional judgement** may request to examine a patient exhibiting COVID- 19 symptoms, using a video chat application connecting the provider's or patient's phone or desktop computer in order to assess a greater number of patients **while limiting the risk of infection** of other persons who would be exposed from an in-person consultation

→ Likewise, a covered health care provider may provide similar telehealth services in the **exercise of their professional judgment** to **assess or treat any other medical condition**, even if not related to COVID-19, such as a sprained ankle, dental consultation or psychological evaluation, or other conditions.

Telehealth Cybersecurity and Privacy Risks

Compliance

Non-compliance with legal and regulatory requirements can lead to reputational, financial, and operational risks.

Organizations may collect sensitive data about individuals such as geolocation data, travel history, etc. Collection of this type of data raises concerns about applications of privacy laws consistently.

Lack of controls within telehealth system may allow users to subvert intended configurations.

Internet of Medical Things (IoMT), Medical device, wearables security

Unauthorized access to devices, resulting in loss of data, device failure, or access to internal network. Malicious actors may look to exploit the ecosystem including new technologies and the cloud.

Data protection

Unauthorized use and disclosure of data, device access, and downstream impact on patient experience.

With more users accessing systems remotely, the risk of Personal Identifiable Information (PII) and Protected health information (PHI) being compromised increases. Some organizations may allow users to download data to a home device or print to a home printer.

Connected devices/wearables increase the volume of data sent to providers. Pictures could be sent as part of virtual visits.

Identity & access management

Unauthorized access to sensitive/confidential data from inadequate authentication methods (e.g., single-factor authentication).

Some technologies may not require users to authenticate with a passcode, token, or biometric data.

Considerations Addressing Cybersecurity and Privacy Risks

1 Virtual health cybersecurity and privacy risk assessment or audit program

- Perform risk assessments over virtual health technologies.
- Review existing policies to assess compliance with cybersecurity and privacy leading practices.
- Review whether appropriate controls are implemented and operating effectively.
- Use analytics to provide deeper insight into virtual health risks:
  - **Leverage Security Information and Event Monitoring (SIEM) tool** to perform exploratory analysis on telehealth/virtual care tools to understand and benchmark areas such as access, connection strength, number of interruptions, compatibility, onboarding capacity.
  - Set up **monitoring and alerts** for the above "areas" to identify and flag anomalies.
  - Analyze if patients comply with **virtual health program requirements** (completed trainings, signed waivers, etc.).
  - Are **medical devices** operating on different networks (like home Wi-Fi?)? Are these networks secure?

2 Collaborate with Information Technology (IT) and business

As new technologies and solutions are identified, such as Hospital@Home, collaborate with IT and business early on so cybersecurity and privacy requirements and controls are embedded within the development lifecycle

3 A path forward

Incorporate virtual health into ongoing audits and risk assessments to confirm ongoing compliance as technologies and regulations change

Practice Standards

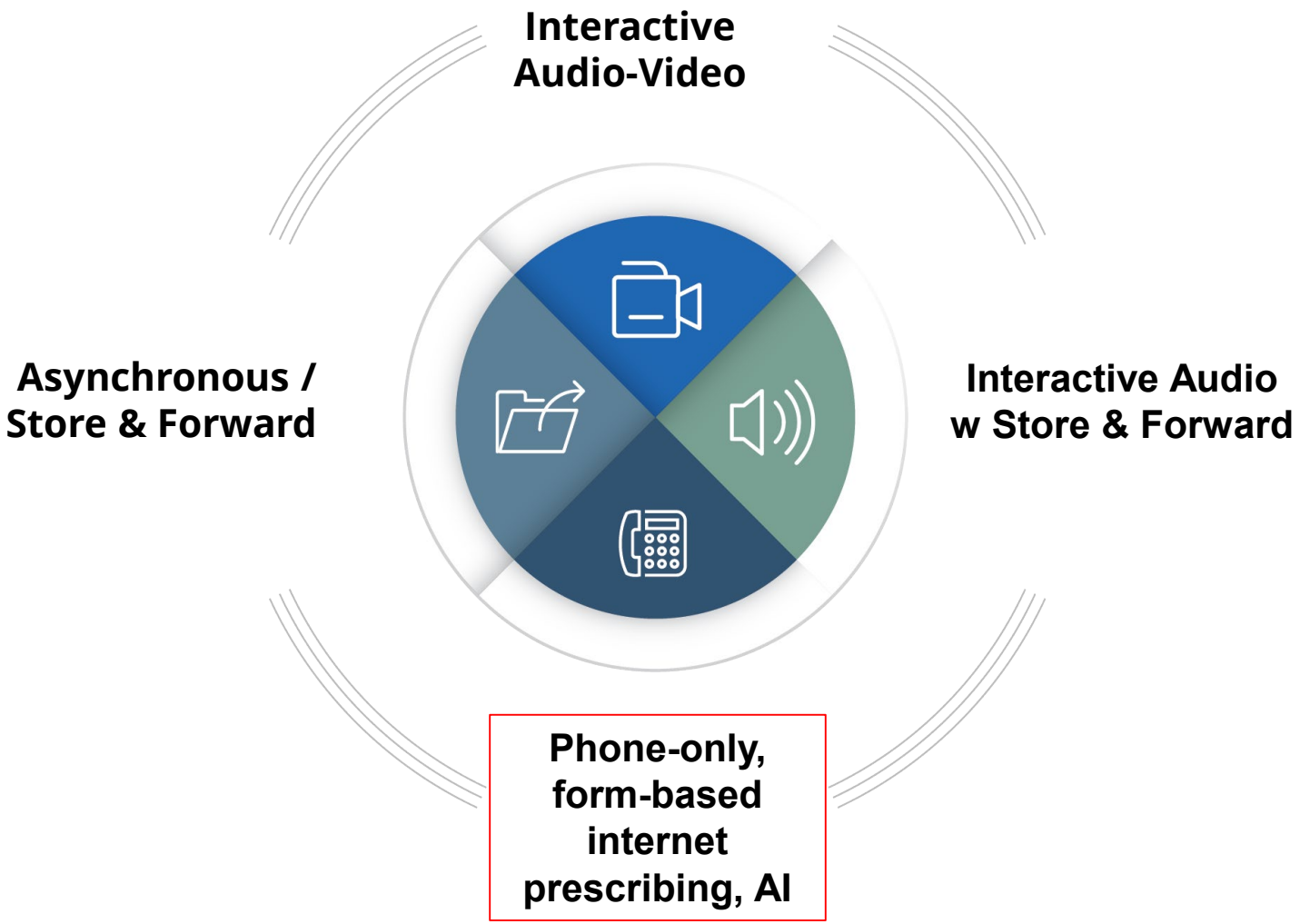
1. Establishing Physician-Patient Relationship
2. Modality of Communication Technology
3. Originating Site Restrictions
4. Patient-Site Telepresenter
5. Remote Prescribing (Non-Controlled Substances)
6. Remote Prescribing (Controlled Substances)
7. Medical Record-Keeping and Record-Sharing
8. Telehealth Informed Consent
9. Sharing Provider's Credentials and Contact Information
10. Special Telehealth Disclosures
11. Verifying the Patient's Identity and Location
12. Referrals for Emergency Services and/or Follow-up Care

Vermont

1 **Establishing Physician-Patient Relationship**

Subject to the limitations of the license under which the individual is practicing, a health care provider licensed in this State may prescribe, dispense, or administer drugs or medical supplies, or otherwise provide treatment recommendations to a patient *after having performed an appropriate examination of the patient in person, through telemedicine, or by the use of instrumentation and diagnostic equipment through which images and medical records may be transmitted electronically*. Treatment recommendations made via electronic means, including issuing a prescription via electronic means, shall be held to the same standards of appropriate practice as those in traditional provider-patient settings. 18 Vt. Stat. Ann. § 9361(b).

Telemedicine Modalities



New Hampshire

2

Modality of Communication Technology

A face-to-face 2-way real-time interactive communication. *See above*, N.H. Rev. Stat. Ann. § 329:1-c.

Vermont/Massachusetts

5 **Remote Prescribing (Non-Controlled Substances)**

6 **Remote Prescribing (Controlled Substances)**

- Providers may issue prescriptions via telemedicine without a prior in-person exam. *See* 18 Vt. Stat. Ann. § 9361(b).
- Massachusetts has no telemedicine-specific practice laws, regulations, or medical board guidance addressing controlled substance prescribing via telemedicine. Under Massachusetts medical practice standards, to be valid, a prescription for a controlled substance shall be issued for a legitimate medical purpose by a practitioner acting in the usual course of his professional practice. *See* Mass. Gen. Laws Ann. ch. 94C, § 19.

Note: Controlled Substances and the Federal Ryan Haight Act

Rhode Island

7 **Medical Record-Keeping and Record-Sharing**

The medical record should include copies of patient-related electronic communications, including patient-physician e-mail, prescriptions, laboratory and test results, evaluations and consultations, records of past care and instructions that are pertinent to the diagnosis and treatment of the patient.[sic] record.

Patient medical records should remain current and accessible for review and be maintained in compliance with applicable state and federal requirements. See Board of Medical Licensure and Discipline Guidelines for the Appropriate Use of Telemedicine and the Internet in Medical Practice.

- The Board guidelines also proscribe requirements for electronic mail communications between physicians and patients, including specifying that "[p]atient-physician e-mail, as well as other patient-related electronic communications that is pertinent to the diagnosis and treatment of the patient should be stored and filed in the patient's medical record."

Connecticut

10 Special Telehealth Disclosures

11 Verifying the Patient's Identity and Location

Special Disclosures

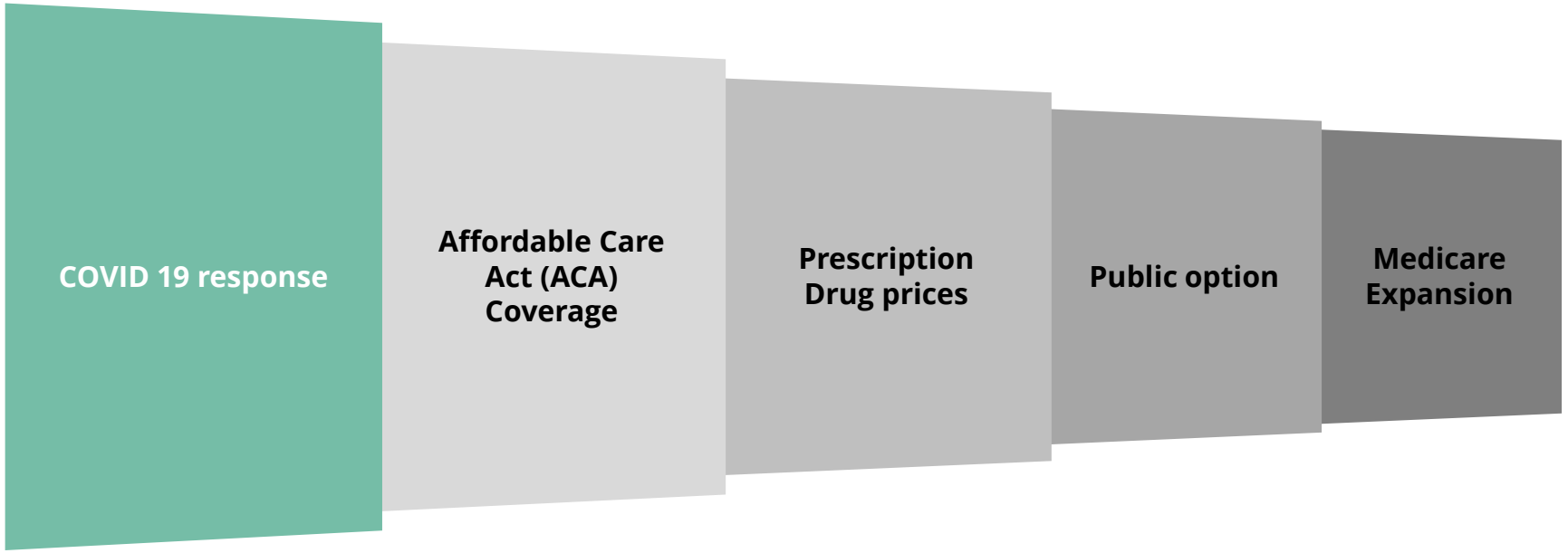
A telehealth provider shall only provide telehealth services to a patient when the telehealth provider . . . (B) has access to, or knowledge of, the patient's medical history, as provided by the patient, and the patient's health record, including the name and address of the patient's primary care provider, if any; and . . . (D) *provides the patient with the telehealth's provider license number and contact information*. See Conn. Gen. Stat. Ann. § 19a-906(b)(1).

Patient ID

Connecticut does not have any patient identity verification requirements.

Compliance Hot Topics Post Covid-19

Key health care priorities of President Biden



Source: https://www.whitehouse.gov/priorities/

DOJ compliance program effectiveness considerations

The DOJ guidance considers three fundamental questions with corresponding topics when evaluating compliance program effectiveness

1. Is the Corporation's Compliance program well designed?	
Policies and Procedures (P&P)	P&Ps should aim to reduce risks identified from the risk assessment. Codes of conduct should detail commitment to comply with federal laws.
Risk Assessment	Companies should identify, assess, and define its risk profile and the degree to which the program devotes appropriate scrutiny and resources to a spectrum of risks.
Training and Communications	Trainings, certifications, and communications should be tailored and conducted periodically to ensure integration within the company.
Confidential Reporting and Investigation	Companies should have an efficient and trusted mechanism to confidentially report misconduct.
Third Party Management	Companies should apply risk-based due diligence to its third-party relationships.
Mergers and Acquisitions ("M&A")	Compliance programs should include comprehensive due diligence of acquisition targets.
2. Is the program being applied earnestly and in good faith?	
Senior and Middle Management	Company leaders set the tone for a culture of compliance.
Autonomy and Resources	Day to day oversight is essential for the effective implementation of compliance programs.
Incentives and Disciplinary Measures	Compliance programs should have established incentives for compliance and disincentives for non-compliance.
3. Does the corporate compliance program work in practice?	
Continuous Improvement, Periodic Testing and Review	Compliance programs should have the capacity to improve and evolve. Internal audit should conduct periodic compliance audits, and the company should also test compliance controls and perform gap assessments.
Analysis and Remediation of Underlying Misconduct	Compliance programs should enable companies to conduct thoughtful root cause analysis of misconduct and timely and appropriate remediation of the root causes.
Investigation of Misconduct	Compliance programs should have a funded mechanism for the timely and thorough investigation of any allegation of misconduct by the company, its employees, or agents.

Source: U.S. Department of Justice, Criminal Division, Fraud Section, Evaluation of Corporate Compliance Programs (Updated June 2020)

Crosswalk between DOJ and OIG Guidance

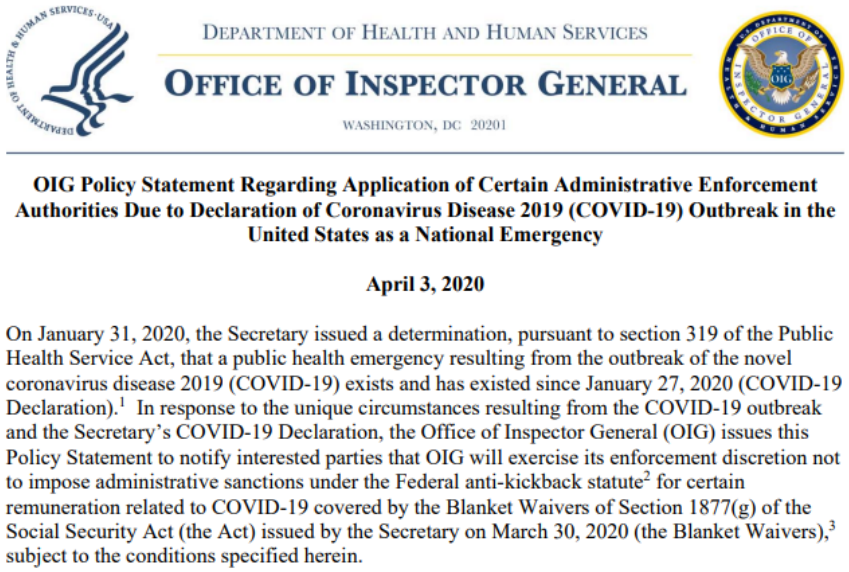
	DOJ Elements	Related OIG Core Elements
1.	Policies and Procedures	Written Standards of Conduct
2.	Senior and Middle Management	Program structure, including Board Oversight and a Compliance Officer
3.	Autonomy and Resources	Program structure, including Board Oversight and a Compliance Officer
4.	Training and Communications	Employee Training and Education Communication Systems
5.	Incentives and Disciplinary Measures	Enforcement
6.	Risk Assessment	Auditing and Monitoring
7.	Analysis and Remediation of Underlying Misconduct	Response and Prevention
8.	Continuous Improvement, Period Testing and Review	Auditing and Monitoring Response and Prevention
9.	Confidential Reporting and Investigation	Non-intimidation and Non-realization
10.	Thirty Party Management	Auditing and Monitoring
11.	Mergers and Acquisitions (M&A)	N/A

Source: U.S. Department of Justice, Criminal Division, Fraud Section, Evaluation of Corporate Compliance Programs (Updated June 2020);
https://oig.hhs.gov/compliance/101/files/HCCA-OIG-Resource-Guide.pdf

Waivers During PHE

- COVID-19 Emergency Declaration Blanket Waivers & Flexibilities for Health Care Providers (44 page summary, 2/19/21 latest rev.)

Stark Blanket Waivers & AKS Policy Statement



DEPARTMENT OF HEALTH AND HUMAN SERVICES

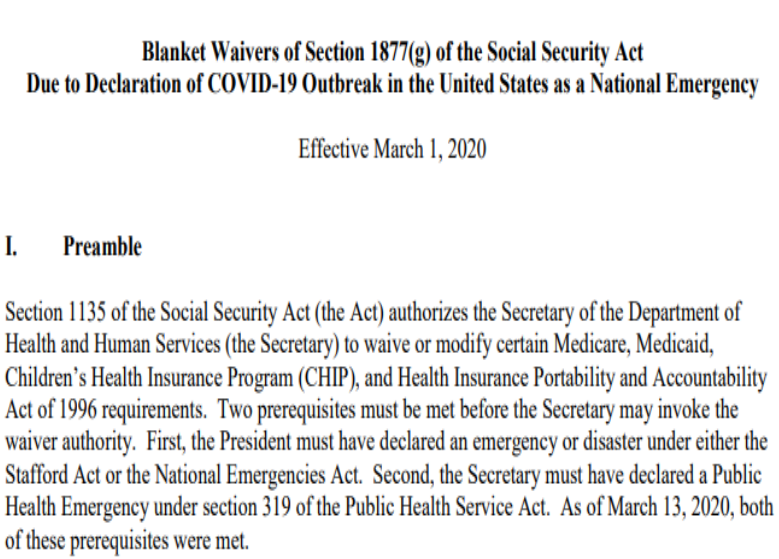
OFFICE OF INSPECTOR GENERAL

WASHINGTON, DC 20201

OIG Policy Statement Regarding Application of Certain Administrative Enforcement Authorities Due to Declaration of Coronavirus Disease 2019 (COVID-19) Outbreak in the United States as a National Emergency

April 3, 2020

On January 31, 2020, the Secretary issued a determination, pursuant to section 319 of the Public Health Service Act, that a public health emergency resulting from the outbreak of the novel coronavirus disease 2019 (COVID-19) exists and has existed since January 27, 2020 (COVID-19 Declaration).[1] In response to the unique circumstances resulting from the COVID-19 outbreak and the Secretary's COVID-19 Declaration, the Office of Inspector General (OIG) issues this Policy Statement to notify interested parties that OIG will exercise its enforcement discretion not to impose administrative sanctions under the Federal anti-kickback statute[2] for certain remuneration related to COVID-19 covered by the Blanket Waivers of Section 1877(g) of the Social Security Act (the Act) issued by the Secretary on March 30, 2020 (the Blanket Waivers),[3] subject to the conditions specified herein.



Blanket Waivers of Section 1877(g) of the Social Security Act
Due to Declaration of COVID-19 Outbreak in the United States as a National Emergency

Effective March 1, 2020

I. Preamble

Section 1135 of the Social Security Act (the Act) authorizes the Secretary of the Department of Health and Human Services (the Secretary) to waive or modify certain Medicare, Medicaid, Children's Health Insurance Program (CHIP), and Health Insurance Portability and Accountability Act of 1996 requirements. Two prerequisites must be met before the Secretary may invoke the waiver authority. First, the President must have declared an emergency or disaster under either the Stafford Act or the National Emergencies Act. Second, the Secretary must have declared a Public Health Emergency under section 319 of the Public Health Service Act. As of March 13, 2020, both of these prerequisites were met.

https://www.cms.gov/files/document/covid-19-blanket-waivers-section-1877g.pdf
https://www.cms.gov/files/document/explanatory-guidance-march-30-2020-blanket-waivers-section-1877g-social-security-act.pdf
https://oig.hhs.gov/coronavirus/OIG-Policy-Statement-4.3.20.pdf

Payments During PHE

- Accelerated and Advance Payment Programs $100B (80% to Hospitals)
- Payroll Protection Program (PPP) and other Loans $520B total; $68B to health care providers
- 20% Increase in inpatient reimbursement for Covid-19 patients
- $40/dose vaccine administration fees
- $178B Provider Relief Fund
  - As of March 31, 2021, the CDC reports that **411,376 providers** have received and accepted PRF payments for a total of **$113B**

Provider Relief Funds

- Coronavirus Aid, Relief, and Economic Security ("CARES") Act. Among many other things, the CARES Act created the Provider Relief Fund ("PRF") Coronavirus Aid, Relief, and Economic Security Act, Pub. L. No. 116-136, tit. VIII, 134 Stat. 281 (2020)
- $178 Billion
- 10-page Terms and Conditions; Attestation
- Policy Memo (9/19/2020)
- Reporting Requirements Policy Update (10/22/20) ("HHS has amended its reporting instructions to provide for the full applicability PRF distributions to lost revenues.")
- 60 pages of FAQs, updated continually (4/1/2021 latest update)
  - There were 45 pages of FAQs when we covered this at HCCA on 9/11/2020, 55 for MHA on 11/5/2020
  - 106 new or modified FAQs in just Oct/Nov.

Provider Relief Funds

New traps:

If a provider returns a Provider Relief Fund payment to HHS, must it also return any accrued interest on the payment? (*Added 10/28/2020, Modified 12/11/2020*)

Yes, for Provider Relief Fund payments that were held in an interest-bearing account, the provider must return the accrued interest associated with the amount being returned to HHS. However, if the funds were not held in an interest-bearing account, there is no obligation for the provider to return any additional amount other than the Provider Relief fund payment being returned to HHS. HHS reserves the right to audit Provider Relief Fund recipients in the future to ensure that payments that were held in an interest-bearing account were subsequently returned with accrued interest.

Provider Relief Funds

What if my payment is greater than expected or received in error? (*Modified 8/4/2020 – and again in an immaterial way on 10/28/2020*)

Providers that have been allocated a payment must sign an attestation confirming receipt of the funds and agree to the Terms and Conditions within 90 days of payment. In accordance with the Terms and Conditions, if you believe you have received an overpayment and expect that you will have cumulative lost revenues and increased costs that are attributable to coronavirus during the COVID-19 public health emergency that exceed the intended calculated payment, then you may keep the payment.

If a provider does not have or anticipate having these types of COVID-19-related eligible expenses or lost revenues equal to or in excess of the Provider Relief Fund payment received, it should reject the payment in Provider Relief Fund Attestation Portal or the Provider Relief Fund Application and Attestation Portal and return the entire payment. Please call the Provider Support Line at (866) 569-3522 (for TYY, dial 711) for step-by-step instructions on returning the payment and receive the correct payment when relevant.

Provider Relief Funds

What if my payment is greater than expected or received in error? (*Modified 12/4/2020*)

If HHS identifies a payment made in error, HHS will recoup the erroneous amount. If a provider receives a payment that is greater than expected and believes the payment was made in error, the provider should contact the Provider Support Line at (866) 569-3522 (for TYY, dial 711) and seek clarification.

Keeping track? That's changing a "Yes" to a "No"

OIG Activities

- 54 Active Work Plan items addressing Covid-19 (not all focusing on providers)
- Just added January and Feb. 2021:
  - Audits of Medicare Part B Laboratory Services During the COVID-19 Pandemic "The series of audits will also focus on aberrant billing of COVID-19 testing during the pandemic."
  - Audit of Home Health Services Provided as Telehealth During the COVID-19 Public Health Emergency

OIG Activities

- PRF-Specific Audits:
  - Audit of CARES Act Provider Relief Funds—General and Targeted Distributions to Hospitals
  - Audit of HRSA's Controls Over Medicare Providers' Compliance with the Attestation, Submitted-Revenue-Information, and Quarterly Use-of-Funds Reporting Requirements Related to the $50 Billion General Distribution of the Provider Relief Fund
  - Audit of CARES Act Provider Relief Funds—Distribution of $50 Billion to Health Care Providers

OIG Activities

- Other Covid-19 Work Plan Activities:
  - Audit of Medicare Payments for Inpatient Discharges Billed by Hospitals for Beneficiaries Diagnosed With COVID-19
  - Audit of CARES Act Provider Relief Funds—General and Targeted Distributions to Hospitals
  - Infection Control and Emergency Preparedness at Dialysis Centers During the COVID-19 Pandemic
  - Use of Medicare Telehealth Services During the COVID-19 Pandemic
  - Medicaid—Telehealth Expansion During COVID-19 Emergency
  - Trend Analysis of Medicare Laboratory Billing for Potential Fraud and Abuse With COVID-19 Add-on Testing
  - Audit of Nursing Homes' Reporting of COVID-19 Information Under CMS's New Requirements

First Prosecutions

- Multiple PPP Loan fraud cases
- First Criminal Indictment for PRF Misappropriation: Amina Abbas, E.D Michigan (1 on 1 Home Health) Feb. 11, 2021
  - HHA already shut down following $1.6MM overpayment demand, did not operate during pandemic, but received $37,656.95 in PRF. Abbas then allegedly misappropriated the funds by issuing checks to her family members for personal use.
  - Small dollar case, extreme facts. OIG & FBI investigated

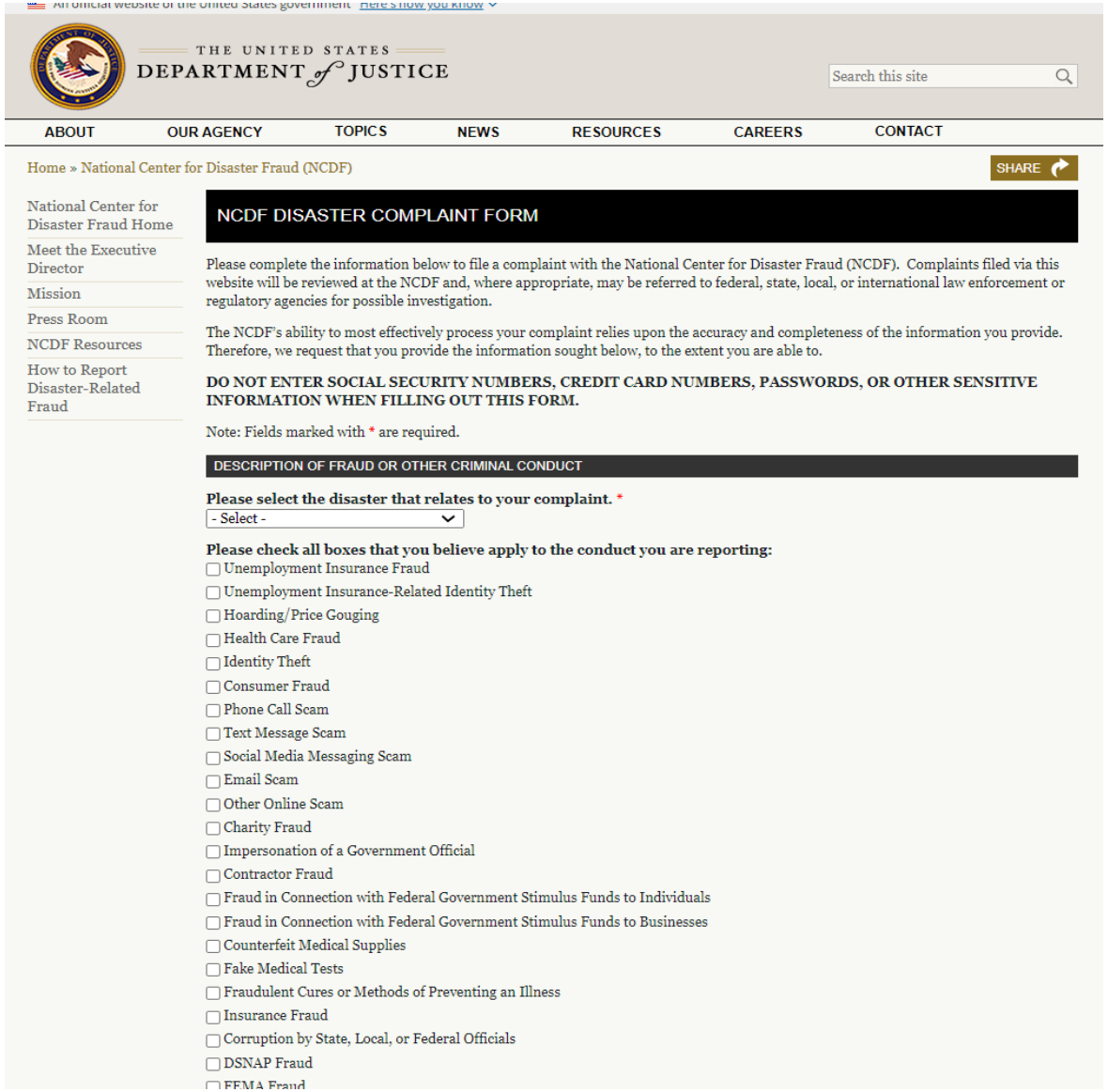
First Prosecutions

- Criminal indictment unsealed on April 7, 2021 in Denver Co.
- Physician, Francis F. Joseph, charged with misappropriating $300,000 in:
  - Paycheck Protection Program
  - Provider Relief Fund
  - Advance & Accelerated Payments

Disaster Fraud Hotline

- "Anyone with information about allegations of attempted fraud involving COVID-19 can report it by calling the Department of Justice's National Center for Disaster Fraud Hotline at 866-720-5721 or via the NCDF Web Complaint Form at: https://www.justice.gov/disaster-fraud/ncdf-disaster-complaint-form."

Disaster Fraud Hotline



An official website of the United States government Here's how you know

THE UNITED STATES DEPARTMENT of JUSTICE

Search this site

ABOUT | OUR AGENCY | TOPICS | NEWS | RESOURCES | CAREERS | CONTACT

Home » National Center for Disaster Fraud (NCDF)

SHARE

- National Center for Disaster Fraud Home
- Meet the Executive Director
- Mission
- Press Room
- NCDF Resources
- How to Report Disaster-Related Fraud

NCDF DISASTER COMPLAINT FORM

Please complete the information below to file a complaint with the National Center for Disaster Fraud (NCDF). Complaints filed via this website will be reviewed at the NCDF and, where appropriate, may be referred to federal, state, local, or international law enforcement or regulatory agencies for possible investigation.

The NCDF's ability to most effectively process your complaint relies upon the accuracy and completeness of the information you provide. Therefore, we request that you provide the information sought below, to the extent you are able to.

DO NOT ENTER SOCIAL SECURITY NUMBERS, CREDIT CARD NUMBERS, PASSWORDS, OR OTHER SENSITIVE INFORMATION WHEN FILLING OUT THIS FORM.

Note: Fields marked with * are required.

DESCRIPTION OF FRAUD OR OTHER CRIMINAL CONDUCT

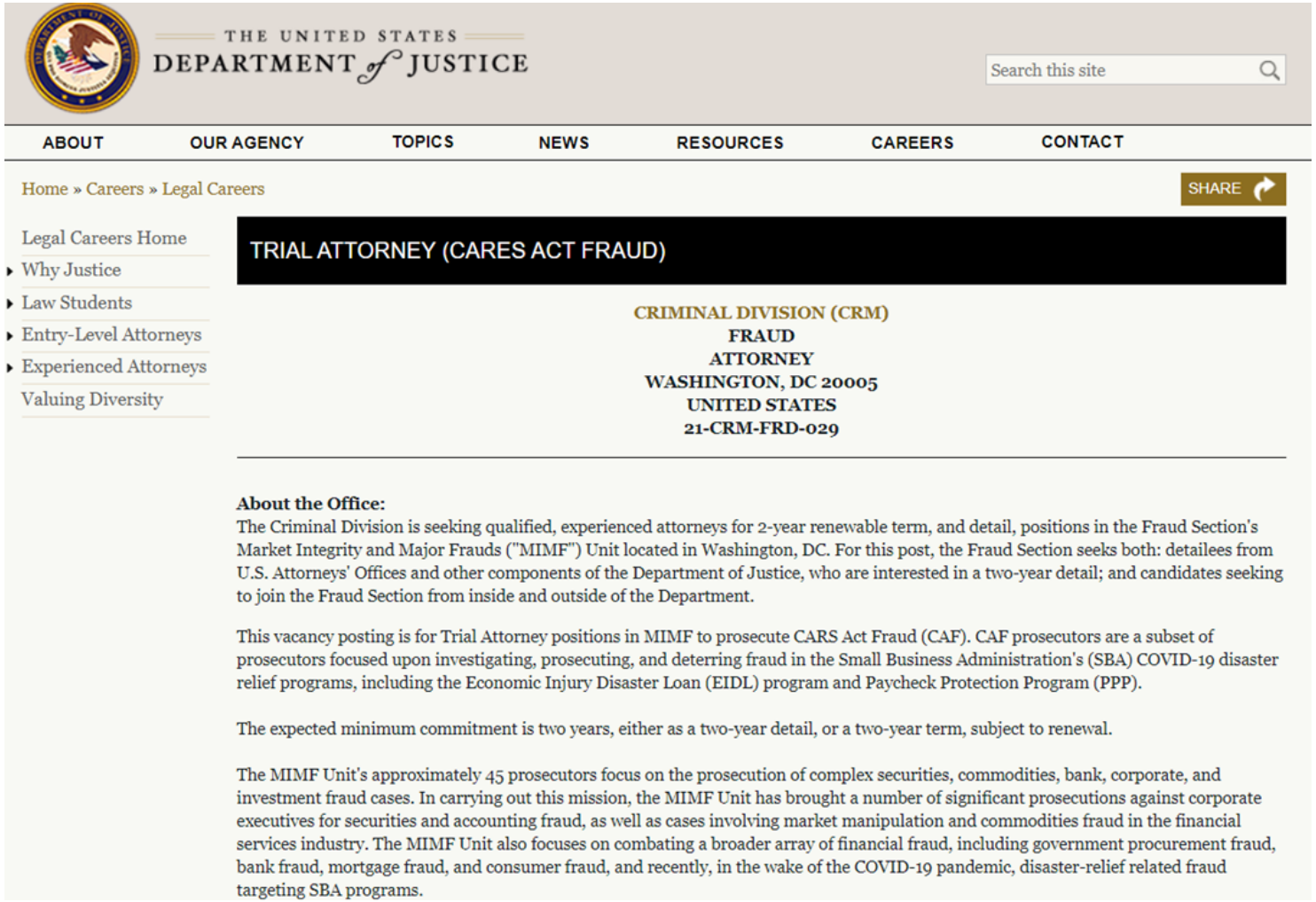
Please select the disaster that relates to your complaint. *

- Select -

Please check all boxes that you believe apply to the conduct you are reporting:

- ☐ Unemployment Insurance Fraud
- ☐ Unemployment Insurance-Related Identity Theft
- ☐ Hoarding/Price Gouging
- ☐ Health Care Fraud
- ☐ Identity Theft
- ☐ Consumer Fraud
- ☐ Phone Call Scam
- ☐ Text Message Scam
- ☐ Social Media Messaging Scam
- ☐ Email Scam
- ☐ Other Online Scam
- ☐ Charity Fraud
- ☐ Impersonation of a Government Official
- ☐ Contractor Fraud
- ☐ Fraud in Connection with Federal Government Stimulus Funds to Individuals
- ☐ Fraud in Connection with Federal Government Stimulus Funds to Businesses
- ☐ Counterfeit Medical Supplies
- ☐ Fake Medical Tests
- ☐ Fraudulent Cures or Methods of Preventing an Illness
- ☐ Insurance Fraud
- ☐ Corruption by State, Local, or Federal Officials
- ☐ DSNAP Fraud
- ☐ FEMA Fraud

DOJ Hiring!



THE UNITED STATES DEPARTMENT of JUSTICE

Search this site

ABOUT | OUR AGENCY | TOPICS | NEWS | RESOURCES | CAREERS | CONTACT

Home » Careers » Legal Careers

SHARE

- Legal Careers Home
- Why Justice
- Law Students
- Entry-Level Attorneys
- Experienced Attorneys
- Valuing Diversity

TRIAL ATTORNEY (CARES ACT FRAUD)

CRIMINAL DIVISION (CRM)
FRAUD
ATTORNEY
WASHINGTON, DC 20005
UNITED STATES
21-CRM-FRD-029

About the Office:
The Criminal Division is seeking qualified, experienced attorneys for 2-year renewable term, and detail, positions in the Fraud Section's Market Integrity and Major Frauds ("MIMF") Unit located in Washington, DC. For this post, the Fraud Section seeks both: detailees from U.S. Attorneys' Offices and other components of the Department of Justice, who are interested in a two-year detail; and candidates seeking to join the Fraud Section from inside and outside of the Department.

This vacancy posting is for Trial Attorney positions in MIMF to prosecute CARS Act Fraud (CAF). CAF prosecutors are a subset of prosecutors focused upon investigating, prosecuting, and deterring fraud in the Small Business Administration's (SBA) COVID-19 disaster relief programs, including the Economic Injury Disaster Loan (EIDL) program and Paycheck Protection Program (PPP).

The expected minimum commitment is two years, either as a two-year detail, or a two-year term, subject to renewal.

The MIMF Unit's approximately 45 prosecutors focus on the prosecution of complex securities, commodities, bank, corporate, and investment fraud cases. In carrying out this mission, the MIMF Unit has brought a number of significant prosecutions against corporate executives for securities and accounting fraud, as well as cases involving market manipulation and commodities fraud in the financial services industry. The MIMF Unit also focuses on combating a broader array of financial fraud, including government procurement fraud, bank fraud, mortgage fraud, and consumer fraud, and recently, in the wake of the COVID-19 pandemic, disaster-relief related fraud targeting SBA programs.