APPENDIX B

HCSC COMPLIANCE PROGRAM
SELECTED HEALTH CARE CRIMINAL AND CIVIL PENALTIES

I. Selected Relevant Statutes and Penalties

A corporation may be prosecuted and held criminally responsible for criminal acts committed by its employees or agents if those acts were committed within the scope of their employment and with the intent to at least partially benefit the corporate business. When the act is within the scope of the employee's authority, the corporation may be liable even if the act is expressly prohibited by corporate policy.

As detailed below, both federal and state governments apply a number of different criminal and civil statutes potentially applicable to the Companies' conduct, the violation of which may result in fines, imprisonment, civil money penalties and business exclusions:

A. Health Care Fraud

1. Federal Health Care Offense Defined: 18 U.S.C. § 24

In 1996, Congress passed a broad new health care and privacy statute commonly referred to as HIPAA. Under this law, a federal health care offense includes a violation of (or conspiracy to violate) a number of specified laws, including ERISA, if related to a health care benefit program. A health care benefit program is defined very broadly as "any public or private plan or contract, affecting commerce, under which any medical benefit, item, or service is provided to any individual, and includes any individual or entity who is providing a medical benefit, item, or service for which payment may be made under the plan or contract."

2. Health Care Fraud: 18 U.S.C. § 1347

This health care fraud offense, created as part of HIPAA, expands significantly the scope of federal criminal jurisdiction in that it applies not just to claims made to public benefits programs, but to those made to private insurers as well. The statute makes it a felony for any person to knowingly and willfully execute or attempt to execute a "scheme or artifice" to defraud any health care benefit program or to obtain any money or property owned by or under the custody or control of any health care benefit program. A conviction for this offense carries an array of possible imprisonment scenarios up to ten years, unless the violation results in serious bodily injury or death, in which case the penalty can rise to twenty years or life, respectively.

3. Embezzlement of Health Care Funds: 18 U.S.C. § 669

This section makes it an offense to embezzle, steal, or intentionally misapply the assets of a health care benefit program. The penalty for violating this statute is dependent on the value of the assets at issue. The possible penalties include a fine and/or imprisonment for up to ten years.

4. Health Care Related False Statements: 18 U.S.C. § 1035

This statute makes it a crime for any person in connection with the delivery of or payment for health care benefits, services or items to falsify or conceal a material fact, to make materially false or fraudulent statements, or to use any materially false documents. A violation of this provision may result in a fine and/or imprisonment for up to five years.

5. Obstruction of Criminal Investigations of Health Care Offenses: 18 U.S.C. §1518

This statute makes it a crime for anyone to willfully prevent, obstruct, mislead, delay or attempt to obstruct the communication of information or records relating to a violation of a federal health care offense to a criminal investigator, including any authorized governmental department or agency. Those convicted may be either fined and/or imprisoned for up to five years.

6. Civil Monetary Penalties Act: 42 U.S.C. §1320a-7a

In the Civil Monetary Penalties Act, Congress established civil monetary penalties that target upcoding, medically unnecessary services, and improper inducements to Medicare and Medicaid beneficiaries. See section H.3 below and 42 C.F.R. § 1003.

7. Health Care Fraud and Abuse Data Collection Program: 42 U.S.C. § 1320a-7e

As part of HIPAA, Congress directed the Secretary for Health and Human Services (HHS) to establish a national health care fraud and abuse data collection program for reporting and disclosing certain final adverse actions taken against health care providers, suppliers and practitioners, and to maintain a database. The database is known as the National Practitioner Data Bank ("NPDB"). This database was originally known as the Health Integrity and Protection Data Base, but both databases were merged in May of 2013.

Through regulation, 42 CFR Pt 60 *et. seq.*, HHS has clarified the reporting requirements of health plans to the database. Most notably, health plans are required to report, among other things, (i) civil judgments against health care providers, suppliers or practitioners related to the delivery of a health care item or service, and (ii) other adjudicated actions or decisions related to the delivery, payment or provision of a health care item or service, against health care providers, suppliers or practitioners. These reporting requirements apply regardless of

whether the civil judgment or other action is subject to a pending appeal. The failure to report such information subjects a health plan to a penalty of up to $22,363 under the Civil Monetary Penalties Act, 42 U.S.C. § 1320a-7a.

8. Eliminating Kickbacks in Recovery Act of 2018 ("EKRA"): 18 U.S.C. § 220.

EKRA, which was incorporated into the omnibus opioid-related legislation (SUPPORT for Patients and Communities Act (P.L. 115-271)) signed into law on October 24, 2018, addresses concerns regarding patient brokering activities relating to treatment for patients addicted to opioids for which some members of Congress believed there was a gap in federal laws. For any services covered by a health care benefit program, EKRA prohibits the knowing and willful soliciting or receiving of any remuneration in return for referring a patient or patronage to a recovery home, clinical treatment facility, or laboratory; or paying or offering any remuneration to induce a referral of an individual to a recovery home, clinical treatment facility, or laboratory, or in exchange for an individual using the services of that recovery home, clinical treatment facility, or laboratory. A health care benefit program includes any government or private health plan, and so is referred to as an "all-payor" statute. Violations are subject to up to fines of up to $200,000, 10 years in jail, or both, for each occurrence. EKRA contains several exceptions, some of which are similar to the federal anti-kickback statute (discussed below). To date, no regulations or interpretative guidance have been issued by the Attorney General on EKRA.

B. Federal Health Care Program Fraud: 42 U.S.C. §§ 1320a-7b(a), (c)

Prior to HIPAA's expansion of federal jurisdiction, Congress had sought specifically to prevent fraud and kickbacks (discussed below) in the operation of the Medicare/ Medicaid programs. In addition to creating new criminal offenses, HIPAA expanded the anti-kickback statute to cover all federal health care programs (defined as any plan or program that provides health benefits, which includes Medicare, Medicaid, and Tricare and excludes the federal employees health benefits program). Federal health care program applicants and providers may be subject to criminal prosecution for, among other things, knowingly making any false statement or misrepresentation of a material fact in any application for any federal health care program benefit, or for use in determining the rights to such benefit or payments.

They also face criminal liability for concealing or failing to disclose one's knowledge of any event that would affect a person's initial or continuing right to receive Medicare/ Medicaid; and knowingly making false statements or misrepresentations with respect to the conditions or operation of any institution, hospital, or health care facility or entity for which certification is required for federal health care program eligibility.

C. Federal Health Care Program Anti-Kickback Statute: 42 U.S.C. § 1320a-7b(b)

Congress specifically sought to prohibit the payment of kickbacks or illegal remunerations in association with the federal health care programs. The "Anti-Kickback Statute" (AKS) prohibits any person from knowingly and willfully offering, paying, soliciting, or receiving any remuneration (including kickbacks, bribes or rebates) directly or indirectly, in return for patient referrals or purchasing, leasing, ordering, arranging for, or recommending any goods, facility, service or item(s) which are reimbursable under federal health care programs. Given the breadth of the statute, there are a number of statutory exceptions and regulatory safe harbors that protect certain types of remuneration from prosecution even if one purpose is to induce or reward referrals. Compliance with these exceptions and safe harbors is not required, however. Arrangements that do not fit within a statutory exception or regulatory safe harbor are subject to a facts and circumstances analysis to determine the potential risks of running afoul of the purposes behind the AKS, which are preventing overutilization, excessive federal health care program costs, corruption of medical decision-making concerning patient care, and unfair competition. A violation of this section will result in fines up to $100,000 and/or up to ten years in prison.

A kickback is not limited to cash referral fees; "in kind" payments for having received special consideration in the purchase of items or in the making of referrals will qualify as a kickback. Examples of possible kickbacks include routine waiver of copayments and deductibles; tickets to sporting events, education materials, educational grants, medical equipment, rebates, and consulting fees offered by health care providers or pharmaceutical drug representatives to physicians, HMOs or hospitals as a quid pro quo for business, etc. Due to the complexity of this law, consult the Company's policies or a Supervisor of the Legal Department for more information regarding the scope of potential kickbacks.

D. False Claims Acts: 18 U.S.C. § 287 and 31 U.S.C. §§ 3729 *et seq*.

Congress passed the criminal False Claims Act ("FCA") at 18 U.S.C. § 287 to punish individuals who undermine or disrupt the operation or integrity of federally funded programs. The statute prohibits making false, fictitious, or fraudulent claims against the federal government. The FCA has been used to prosecute a wide range of frauds, including Medicare, Medicaid, and Social Security fraud, claims for services not rendered under special government programs, false claims for worker's compensation, and false claims to insurers who then submitted claims to the federal government. Criminal penalties include fines and up to ten years incarceration.

Most claims that would be actionable under the FCA could also be prosecuted under the Federal health care program Civil Monetary Penalties Act, 42 U.S.C. **§** 1320a-7a, and the Federal health care program fraud and abuse statute, 42 U.S.C. **§** 1320a-7b. In addition, under the civil False Claims Act, a person may be liable for improperly avoiding an obligation to refund money to the federal government (such as under rules governing refunds of Medicare and Medicaid overpayments).

The civil FCA (at 31 U.S.C. §§ 3729 et seq.) defines "knowingly" to mean the person (1) has actual knowledge that the information is false; (2) acts with deliberate ignorance of the truth or falsity of the information; or (3) acts in reckless disregard of the truth or falsity of the information. This standard requires more than mere negligence and something less than specific intent to disobey the law. Gross negligence or deliberate indifference to the falsity of the information must be shown.

In addition to direct prosecution of civil or criminal false claims by the Justice Department, *qui tam* or whistleblower suits can be brought under the civil False Claims Act. 31 U.S.C. § 3730. Such suits are brought in the name of the government and allow the whistleblower to recover 15 to 25 percent of the government's recovery resulting from that individual's information, or up to 30 percent if the government does not intervene and take over litigating the case. The civil False Claims Act provides for penalties of $12,537to $25,076per false claim (periodically adjusted for inflation) plus three times the amount of damages the government sustained. **In addition to civil claims under the federal False Claims Act, most states and some cities have their own False Claims Act which apply to claims for false, fictious or fraudulent claims for payment to the applicable governmental entity. *See, e.g.*, The New Mexico Medicaid False Claims Act, N.M. Stat. Ann. §§ 27-14-1 et seq.**

E. <u>Privacy, Security, and Breach Notification Standards</u>: The Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d) and its implementing regulations at 45 C.F.R. Parts 160, 162, and 164; as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub Law 111-5, § 13001, et seq.; 42 U.S.C. § 1320c-9(c); State Insurance Data Security Laws

HIPAA's privacy and security requirements apply to PHI which, generally, means any identifiable information that is created or received by a health care provider, health plan, or health care clearinghouse, and that relates to the past, present, or future health of an individual. HIPAA regulates "covered entities," which are health plans, health clearinghouses (i.e., entities that process non-standardized health information received from a covered entity into standardized data elements), and health care providers that conduct certain financial and administrative transactions electronically (e.g., electronic billing and funds transfers).

HIPAA mandates that every covered entity have a "business associate contract" with its business associates containing certain mandated privacy, security, and breach notification provisions. Broadly, a business associate is any entity that creates, receives, maintains, or transmits PHI on behalf of a covered entity for a function regulated by HIPAA, or that provides certain services to a covered entity (such as management or administrative

services) that require the disclosure of PHI to the entity. .If a covered entity knew of a pattern of activity or practice that constituted a material breach of the business associate contract terms, HIPAA requires the covered entity to take reasonable steps to cure the breach. If such steps prove unsuccessful, the covered entity must terminate the business associate contract, if feasible.

On January 25, 2013 HHS published a final rule modifying HIPAA and implementing statutory amendments under HITECH to strengthen the privacy and security protection for an individual's health information. This rule also modified breach notification requirements under HITECH and strengthened privacy protections for genetic information. Under the rule, business associates are now directly liable for noncompliance with certain HIPAA requirements.

On December 10, 2021, HHS published proposed changes to the HIPAA Privacy Rule. The proposed changes include (a) the strengthening of individuals' rights to access their own health information, (b) improving information sharing for care coordination and case management for individuals, (c) facilitating greater family and caregiver involvement in the care of individuals experiencing emergencies or health crises, (d) enhancing flexibilities for disclosures in emergency or threatening circumstances, and (e) reducing administrative burdens associated with HIPAA compliance. A final rule has not yet been published.

HIPAA grants HHS authority to assess civil money penalties ("CMPs") against covered entities and their business associates for a violation of the HIPAA privacy, security, and breach notification provisions within six (6) years of the date on which the violation occurred. HIPAA provides for four different CMP tiers that depend on the covered entity's or business associate's level of culpability: (1) lack of knowledge; (2) reasonable cause; (3) willful neglect, if the violation is corrected within 30 days; and (4) willful neglect, if the violation is uncorrected within 30 days. HIPAA also specifies cumulative annual limits on CMPs that HHS may assess within each penalty tier against a covered entity or business associate for multiple violations of an identical HIPAA provision. On April 26, 2019, HHS issued a "Notice of Enforcement Discretion Regarding HIPAA Civil Money Penalties" to inform the public that going forward, the agency will exercise enforcement discretion in applying revised cumulative annual CMP limits for identical HIPAA violations to each penalty tier. These revised annual limits better align with HITECH's statutory language and, depending on the penalty tier, range from $25,000 to $1.5 million. Relatedly, in its Fiscal Year 2020 budget request, the HHS Office for Civil Rights ("OCR"), which enforces HIPAA, announced its intention to largely self-fund its HIPAA mission through enforcement recoveries, with prior HIPAA appropriations to be directed to OCR's Conscience and Religious Freedom Division. Accordingly, OCR investigators and regional offices may be incentivized to obtain more and larger HIPAA enforcement recoveries, subject to the above-described revised cumulative annual limits.

In addition to federal data security requirements, the National Association of Insurance Commissioners ("NAIC") released the Insurance Data Security Model Law at the end of 2017, and several states have enacted the Model Law or related legislation. These state

laws establish minimum requirements for insurers' data security programs, including requiring insurers to report cybersecurity events to the insurance commissioner within specified timeframes (which vary by state). The state laws generally rely on existing penalty provisions set forth in the state insurance code in establishing penalties for noncompliance.

Finally, 42 U.S.C. § 1320c-9(c) also makes it a crime to unlawfully disclose confidential patient information by an entity engaged in peer review of quality management and utilization if such disclosure is not mandated by statute or regulation.

F. General Crimes Relevant to Health Care Providers

1. False Statements: 18 U.S.C. § 1001

One of the statutes mostly commonly used to prosecute fraud, including health care related frauds, is the prohibition against false statements or misrepresentations with regard to "any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States". This statute applies to those statements, either oral or written, sworn or unsworn, made by any provider or employee who falsifies or conceals any material fact; makes any materially false statements or representations; or makes or uses any materially false documents or writings.

Because the defendant must make a false statement both "knowingly and willfully," it should be noted that the intent requirement of §1001 is higher than that required under §287 (False Claims). The fraudulent statements need not be made directly to the federal government to be subject to prosecution. Each offense carries potential imprisonment of up to five to 8 years and fines of up to $250,000 for individuals and $500,000 for corporations.

2. Obstruction of Justice: 18 U.S.C. §§ 1512, 1519, 1520

These provisions prohibit corruptly destroying documents or other evidence (or persuading others to destroy documents or other evidence) with the intent to obstruct an official proceeding. Depending on the circumstances, maximum penalties may include a fine and/or a term of imprisonment of up to 20 years.

Additionally, accountants who fail to retain the audit or review "workpapers" of a covered audit for a period of 5 years can be found guilty of a felony, punishable by up to ten years imprisonment. "Workpapers" are those documents necessary to explain and substantiate the work performed as part of the audit or review. This provision, codified at 18 U.S.C. § 1520, imposes fines and up to a 10-year prison term on any person who "knowingly and willfully" violates this retention requirement.

3. **Retaliation: 18 U.S.C. § 1513**

Under previous law, there was no explicit protection from retaliation for an individual who provides truthful information to a law enforcement officer concerning the commission or possible commission of a federal offense. However, subsection (e) of 18 U.S.C. §1513 now creates a felony offense for any person who knowingly takes any action, with intent to retaliate, that is harmful to a person who provided such information concerning a federal offense. A violation of this statute may result in fines and/or up to ten years in prison.

4. **Money Laundering: 18 U.S.C. § 1956**

The addition to the money laundering statute of health care fraud makes it a crime to launder monetary instruments, specifically (a) to conduct or attempt to conduct a financial transaction involving property known to be the proceeds of an unlawful activity; (b) to transport or attempt to transport funds intending to promote an unlawful activity or knowing that the funds are proceeds of an unlawful activity; or (c) to conduct or attempt to conduct a financial transaction with proceeds of, or represented to be of, an unlawful activity with the intent either to promote the unlawful activity, conceal the property, or avoid a reporting requirement under state or federal law. Here, the "unlawful activity" now includes any federal health care offense. The penalties for each of these violations vary but do not exceed a fine in the amount of $500,000 or twice the value of the property involved and/or imprisonment for up to twenty years.

5. **Conspiracy: 18 U.S.C. §§ 371 and 286**

A conspiracy is a group of two or more persons who have agreed together to commit an illegal act. The agreement between two or more conspirators to accomplish an illegal objective is the very essence of a criminal conspiracy. The conspiratorial agreement does not need to be formal or detailed, nor does it even have to be expressly stated. A tacit understanding of the agreement will suffice. Proof of the agreement between conspirators is usually shown by a defendant's actions.

The general federal conspiracy statute (18 U.S.C. **§** 371) prohibits combinations of two or more persons to violate any law of the United States or to defraud the United States or any government agency. The maximum penalty is five years imprisonment and/or a fine. Under 18 U.S.C. **§** 286, it is unlawful to conspire to make false claims on the government. The maximum penalty for §286 is ten years imprisonment and/or a fine. The conspiracy or agreement itself constitutes a crime separate and distinct from the actual crime committed by any of the conspiracy's members. For example, if two persons conspire to defraud someone and they use the mails to do so, they have committed two crimes: conspiracy and fraud. Even if the fraud never occurs, or even if the fraud scheme is unsuccessful, the conspirators may still be prosecuted for criminal conspiracy.

6. Insurance Business Affecting Interstate Commerce: 18 U.S.C. §§ 1033 and 1034

In 1994, Congress made a number of acts involving the insurance industry federal crimes where the business "affects interstate commerce." Thus, frauds, false statements, embezzlement, deception of auditors and false book entries, among other acts, all carry criminal penalties of imprisonment for up to ten years, and in cases where it jeopardized the safety and soundness of an insurer, up to fifteen years. Section 1033 also requires those convicted of felonies involving breach of trust or dishonesty, to obtain written consent of insurance regulatory officials before engaging in the insurance business. Finally, Section 1034 gives the government injunctive relief and sets forth civil penalties of up to $50,000 for each violation or the amount of compensation which the violator received or offered, whichever is greater.

7. Major Government Fraud: 18 U.S.C. § 1031

In 1988, Congress expanded its antifraud remedies with this criminal statute focusing on schemes to defraud the United States or to obtain money or property by false or fraudulent representations as a prime contractor to the government or a sub-contractor or supplier to a prime government contractor where "the value of such grant, contract, subcontract, subsidy, loan, guarantee, insurance, or other form of Federal assistance, or any constituent part thereof" is $1 million or more. Criminal fines range up to $10,000,000 and imprisonment up to 10 years, or both. The statute also authorizes payments by the Justice Department of up to $250,000 to persons furnishing information relating to a possible Section 1031 prosecution.

8. Mail and Wire Fraud: 18 U.S.C. §§ 1341 and 1343

If a person or entity devises a scheme to commit fraud and utilizes the United States mail or interstate wires (e.g., telephone, facsimile, or electronic mail) to help the fraud along (e.g., mailing a false document to the recipient or making a misrepresentation to a potential customer over the phone in another state), then such fraud - regardless of whether the government or a private citizen was the intended victim - is subject to federal prosecution as a mail or wire fraud. The elements of mail and wire fraud are: (1) intentionally devising or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent, pretenses, representations or promises; and (2) using or causing the use of mails or interstate wires in furtherance of the scheme.

In 2002, Congress passed 18 U.S.C. §1349, which provides that attempts and conspiracies to commit the substantive Federal fraud offenses (including health care fraud - 18 U.S.C. §1347) will have the same punishment as the substantive crime. While the penalty had been five years imprisonment, and a variety of possible fines, the federal mail and wire fraud statutes were amended to increase the maximum penalty to 20 years imprisonment.

9. State Benefits and Medicaid Fraud Laws

In addition to federal laws, states have their own criminal laws prohibiting state benefits fraud or Medicaid fraud. Unlike the federal statutes, however, it is not necessary to use the mail or interstate wires to be criminally prosecuted. The following is a summary of some of the state laws.

a. Illinois: State Benefits Fraud: 720 ILCS 5/17-6

In Illinois, a person is guilty of state benefits fraud if he or she obtains or attempts to obtain money or benefits from the state through the knowing use of false identification documents, or through knowing misrepresentation of his age, place of residence, number of dependents, marital or family status, employment status, financial status, or other material fact upon which his or her eligibility for benefits may be based.

b. Oklahoma: False Claim for Payment of Public Funds or on Employment Application: 21 Okla. Stat. §§ 358, 359

Oklahoma statutes provide for a criminal offense when any person knowingly presents a "false, fictitious or fraudulent claim for payment of public funds upon or against the State of Oklahoma, or any department or agency thereof." Such an offense is considered a felony and punishable by a fine of up to $10,000 or by imprisonment of up to two years, or both.

The statute also prohibits anyone applying for employment with the state of Oklahoma to knowingly make a "materially false, fictitious or fraudulent statement or representation on an employment application." This offense is a misdemeanor and punishable by a fine of up to $1,000 or by imprisonment of up to one year, or both.

c. Texas: False Claims & Anti-Kickback Law; Medicaid Fraud: Tex. Human Res. Code § 32.039, § 36.001 et seq.

Texas law generally provides that it is unlawful to knowingly or intentionally make false statements of a material fact, or to fail to disclose a material fact, in relation to a Medicaid application, benefit, payment or eligibility requirement. Tex. Human Res. Code §§ 36.001 et seq. Related fraudulent activities are also prohibited, such as converting Medicaid benefits for use by persons other than the intended recipient, making false statements regarding facilities that are certified by Medicaid, or presenting false claims for payment, among other activities. The Texas Medicaid Fraud Prevention statute contains civil damage, injunctive, and suspension remedies. There are also special provisions prohibiting managed care

organizations from engaging in certain fraudulent or wrongful conduct. Tex. Human Res. Code § 32.039.

d. <u>New Mexico: Medicaid Fraud Act</u>:
N.M. Stat. Ann. §§ 30-44-1 et seq.

The New Mexico Medicaid Fraud Act, N.M. Stat. Ann. § 30-44-1 et seq., criminalizes a variety of behavior relating to the misuse of program funds. The Act prohibits the paying, soliciting, offering or receiving of kickbacks and bribes, as well as any rebates for referring a recipient to a provider. N.M. Stat. Ann. § 30-44-7. Under the Act, it is also illegal to pay, solicit, offer or receive anything of value with the intention of retaining it and knowing it to be in excess of amounts or rates authorized under the program for the provision of treatment, services or goods. In addition, the Act criminalizes the conduct of individuals and entities that provide below-quality treatment, services or goods with the intent that a claim be relied upon for the expenditure of public money. Related behavior, such as presenting false claims, making false or fraudulent representations, and engaging in intentionally deceptive marketing practices also violates the New Mexico Medicaid Fraud Act. Depending upon the value of the benefit improperly provided and the extent of any physical or psychological harm suffered, a violation of the New Mexico Medicaid Fraud Act can range from a petty misdemeanor to a second degree felony. An entity that commits Medicaid fraud is subject to a fine of not more than $50,000 for each misdemeanor and not more than $250,000 for each felony. N.M. Stat. Ann. § 30-44-7.

e. <u>Montana: False Claim to Public Agency:</u>
Mont. Code Ann. § 45-7-210

In Montana, a person commits a false claim to a public agency if the person knowingly presents for allowance, for payment, or for the purpose of concealing, avoiding, or decreasing an obligation to pay a false or fraudulent claim, bill, account, voucher, or writing to a public agency, public servant, or contractor authorized to allow or pay valid claims presented to a public agency. A person convicted of an offense under this section shall be fined not to exceed $1,500 or imprisoned in the county jail for a term not to exceed 6 months, or both. If a false or fraudulent claim is knowingly submitted as part of a common scheme or if the value of the claim or the aggregate value of one or more claims exceeds $1,500, a person convicted of an offense under this section shall be fined not to exceed $10,000 or imprisoned in the state prison for a term not to exceed 10 years, or both.

10. Program Embezzlement: 18 U.S.C. § 666

Embezzlement is the wrongful or willful taking of someone else's money or property by one who lawfully came into its possession or control. One common example of embezzlement occurs when an employee working in collections "skims" money from customer payments that were made to his or her employer. Embezzlement differs from larceny in that the embezzler's original possession of the property is lawful or is pursuant to the consent of the owner. The federal program embezzlement statute prohibits (1) any agent of any agency, government, or organization (2) that received benefits in excess of $10,000 in the previous twelve months from a "Federal program" (3) from embezzling, stealing, obtaining by fraud, corruptly solicits, demands or accepts anything of value with the intent to influence, or converting to one's use without authority (4) property in excess of $5,000 that is owned or controlled by such agency, government, or organization. A violation of this statute may result in fines and/or up to ten years in prison.

11. Obstruction of Federal Audit: 18 U.S.C. § 1516

Congress made it an offense to intentionally influence, obstruct or impede any federal auditor performing duties relating to the audit of a person, entity or program receiving more than $100,000 of United States funds in any one year. The funds need not come directly from the federal government, as where an entity subcontracts with another who receives federal contract funds.

12. International Emergency Economic Powers Act ("IEEPA"): 50 U.S.C. 1701 § et. seq.

The IEEPA authorizes the President to regulate international commerce after declaring a national emergency in response to any unusual and extraordinary threat to the United States which has its source in whole or substantial part outside the United States. IEEPA authorizes the President to impose economic sanctions on persons and entities posing an "unusual and extraordinary" threat to the national security, foreign policy, or economy of the United States. IEEPA serves as the authority for imposition of U.S. sanctions administered and enforced by the U.S. Department of Treasury, Office of Foreign Assets Control ("OFAC"). IEEPA provides for civil and criminal penalties for violation of its provisions. Under IEEPA, OFAC may impose civil penalties up to the greater of $330,947 or twice the amount of the underlying transaction, per violation. A person who willfully commited, willfully attempts to commit, willfully conspires to commit, or aids or abets in the commission of an unlawful act in violation of IEEPA may be fined not more than $1 million, imprisoned for up to 20 years, or both.

a. Sanctions Administered by OFAC and Related Penalties

IEEPA serves as the principal statutory authority for most OFAC sanctions programs. OFAC administers and enforces economic and trade sanctions generally

based on U.S. foreign policy and national security objectives, including combatting terrorism, narcotics trafficking, and proliferation of weapons of mass destruction. OFAC administers various sanctions programs based on statutes, regulations, and executive orders which target certain foreign governments, individuals, entities, and activities. OFAC's sanctions programs may impose comprehensive restrictions on doing business in certain countries or regions or may target certain designated persons or activities. OFAC currently enforces comprehensive sanctions against Cuba, Iran, North Korea, Syria, the Crimea Region of Ukraine, Donetsk People's Republic ("DNR") Region of Ukraine, and Luhansk People's Republic ("LNR") Region of Ukraine. In addition, OFAC imposes targeted sanctions against designated individuals and entities on its Specially Designated Nationals ("SDN") List. U.S. persons are generally prohibited from dealing with SDNs and the assets of SDNs are frozen. In recent years, OFAC has designated certain individuals as SDNs for engaging in fentanyl and opioid trafficking, as well as entities facilitating such trafficking.

G. Sanctions Relevant to Medicare Advantage Organizations and Part D Plan Sponsors:

42 U.S.C. §§ 1395w-27(g)(1) - (4), (h); 42 U.S.C. § 1395w–151(b)

1. Program Violations. The HHS Secretary may impose sanctions on a Medicare Advantage (MA) organization or Part D Plan Sponsor (collectively, "MA organization") in a number of situations. In particular, the Secretary may impose sanctions if he or she determines that the MA organization: (1) fails substantially to provide medically necessary items and services that are required (under law or under the contract); (2) imposes excess premiums on Enrollees; (3) expels or refuses to re-enroll an individual in violation of the related MA program provisions; (4) does anything to deny or discourage enrollment (except as permitted) by eligible individuals with the organization whose medical condition or history indicates a need for substantial future medical services; (5) misrepresents or falsifies information that is furnished to the Secretary, to an individual, or to any other entity; (6) fails to comply with the applicable requirements relating to provider participation and balance billing; (7) employs or contracts with an excluded entity or individual; (8) enrolls an individual in an MA plan, or transfers an individual from one plan to the other, without prior consent; (9) fails to comply with applicable marketing restrictions; or (10) employs or contracts with an individual or entity who engages in the conduct described above.

2. Remedies for Program Violations. In addition to any other remedies authorized by law, the Secretary may impose any of the following sanctions: civil money penalties of up to $42,788 for most violations (($171,156 in some instances) and/or suspension of marketing, enrollment, or payment. In addition, the Secretary has authority under some circumstances to terminate a contract for program violations. For less significant noncompliance, CMS may issue a notice of

noncompliance or other type of notice. Civil money penalties, sanctions, and less significant compliance notices all may impact an MA organization's past performance evaluation, thereby limiting options for the MA organization to expand product lines or service area.

H. The Possible Consequences of Unlawful Conduct

Some of the federal statutes listed above and most of their state statutory counterparts are felony offenses. For individuals, convictions can result in a substantial term of imprisonment and/or fines and restitution. As an organization, HCSC is obviously not subject to imprisonment. In the event of criminal conviction, however, an organization can be held liable for enormous fines and restitution. For example, in 2002, one pharmaceutical drug company was found guilty and made to pay $875 million. Many other such examples often occur. Criminal misconduct committed by an employee could also subject the organization to additional civil penalties that could be more burdensome than a criminal conviction.

1. Exclusion from Federal Programs: Any provider, health care facility, or claims processor, including HCSC, is subject to a five-year mandatory exclusion from receiving federal health care program payments or reimbursements in the event the Company, provider or health care facility is convicted of a criminal offense related to the delivery of an item or service under federal health care programs. 42 U.S.C. **§** 1320a-7(a).[1]

"Permissive" exclusion is also a possibility under 42 U.S.C. **§** 1320a-7(b). A provider, health care facility or claims processor may, at the discretion of the Secretary for the Department of Health and Human Services, be subject to a period of exclusion from receiving federal health care program payments or reimbursements for other criminal violations and civil infractions. For HCSC, the most pertinent criteria for permissive exclusion include: (1) conviction of a criminal offense under state or federal law relating to fraud, theft, embezzlement, breach of fiduciary responsibility or other financial misconduct connected with a program operated or financed in whole or in part by any government agency; (2) conviction for obstructing an investigation or audit; and (3) engaging in fraud, kickbacks or any other act proscribed by the Anti-Kickback Statute. Related provisions for debarment and suspension from participation in federal health care programs are found in the Federal Acquisition Regulations, FAR 9.406 and 9.407.

[1] This refers to subsection (a), the "Mandatory Exclusion" provisions of 42 U.S.C. §1320a-7, "Exclusion of certain individuals and entities from participation in Medicare and State health care programs," which is not to be confused with 42 U.S.C. § 1320a-7a, which is the Civil Monetary Penalty Statute, referenced in section 3, below. Similarly, any reference within this section to 1320a-7(b) refers to subsection (b) of the same exclusion statute (42 U.S.C. § 1320a-7) and not 42 U.S.C. § 1320a-7b, the federal criminal health care fraud statute, which includes the Anti-Kickback Statute.

The Balanced Budget Act of 1997 (111 Stat. 251) broadened the exclusion period for individuals that have been subject to mandatory exclusion under 42 U.S.C. **§** 1320a-7(a). Their exclusion shall be (i) 10 years if the person has been convicted of *one* prior offense for which exclusion may be imposed; and (ii) permanent if the person has been convicted of *two* prior offenses for which exclusions may be imposed. 42 U.S.C. § 1320a-7(c)(3)(G).

The Balanced Budget Act of 1997 also granted the Secretary of the Department of Health and Human Services ("HHS") the authority to refuse to enter into a Medicare agreement with a physician or supplier who has been convicted of a state or federal felony that the Secretary deems inconsistent with the best interest of program beneficiaries (42 U.S.C. **§** 1395u(h)).

2. Debarment: HCSC acts as a third-party administrator for hundreds of governmental health plans, such as the State of Illinois and the City of Chicago. While the provisions vary, most cities and states – including those in HCSC's five states – prohibit contracting between the city or state and an entity which has sustained certain types of felony conviction. Accordingly, a felony conviction of HCSC may preclude it from retaining contracts with its government health plans.

For instance, in Illinois, "[u]nless otherwise provided, no person or business convicted of a felony shall do business with the State of Illinois or any State agency, or enter into a subcontract, from the date of conviction until 5 years after the date of completion of the sentence for that felony, unless no person held responsible by a prosecutorial office for the facts upon which the conviction was based continues to have any involvement with the business." 30 ILCS 500/50-10. In New Mexico, "[t]he causes for debarment or suspension occurring within three years of the date final action on a procurement is taken include but are not limited to the following… conviction of a bidder, offeror or contractor under state or federal statutes related to embezzlement, theft, forgery, bribery, fraud, falsification or destruction of records, making false statements or receiving stolen property or for violation of federal or state tax laws." N.M. Stat. Ann. § 13-1-178. *See also* 34 Tex. Admin. Code § 10.585 (Texas); Okla. Admin. Code § 260:115-3-23 (Oklahoma); Mont. Code Ann. § 18-4-241 (Montana).

3. <u>Civil Monetary Penalties</u>: In addition to the criminal statutes and penalties noted above, a health care provider may also be subject to both private lawsuits and other governmental sanctions for engaging in unlawful conduct. For example, the Civil False Claim Act, 31 U.S.C. § 3729 *et seq.*, described above, provides for treble damages and penalties of not less than $11,181 and not more than $22,363 per claim for any false or fraudulent claim for payment submitted to the federal government. False or fraudulent federal health care program claims for health care related items or services are also subject to harsh civil penalties under the Civil Monetary Penalties ("CMP") Act, 42 U.S.C. § 1320a-7a.

The CMPAct gives the OIG an enforcement tool analogous to the False Claims Act. In fact, legislative enhancements brought the penalties available under the CMP Act in line with those provided by the FCA. The statute allows the OIG to impose CMPs on an individual or entity that has committed one of several enumerated acts of fraud and abuse or billing/coding violations, including but not limited to the submission of claims for:

- items or services that the person knows or should know were not provided as claimed;
- items or services that the person knows or should know are false or fictitious; and
- physician's services provided by a person not licensed as a physician.

The statute also imposes civil monetary penalties for patterns of upcoding or the provision of medical or other items or services that are not medically necessary, and for improper remuneration likely to influence a beneficiary's choice of provider. The amount of potential civil monetary penalties is adjusted periodically for inflation as published in a table of the Code of Federal Regulations at 45 C.F.R. 102.3. . The government may also seek to assess penalties under the CMP Act of up to three times the amount improperly claimed for each time or service.

The Balanced Budget Act of 1997 ("BBA '97") created civil monetary penalties for anti-kickback violations, thus providing an alternative to the harsh criminal penalties and exclusion options previously available for such infractions. Individuals or entities that violate the anti-kickback law now confront a maximum $100,000 penalty and damages of up to three times the amount of remuneration involved in the prohibited activity.

HIPAA also gave the OIG the authority to impose CMPs on individuals who have an ownership interest in or control of an entity that has been excluded from federal health care programs and who knows or should know of the action creating the basis for the exclusion. Civil monetary penalties may likewise be imposed against an officer or managing employee (e.g., an office manager) of an excluded entity.

BBA '97 likewise created a civil monetary penalty for persons or entities that arrange or contract (by employment or otherwise) with an individual or entity that the person or entity knows or should know is excluded from a federal health care program. This provision will require physicians to exercise even greater care in doing business with other individuals and entities in the health care delivery and payment system. Violations will involve damages of up to three times claimed and a civil money penalty of $22,427 per claim (as of the 2022 inflation adjustment). *See* 42 U.S.C. § 1320a-7a(a)(6); 45 C.F.R. 102..

Further, a civil money penalty of up to $38,159 is imposed against a health plan that fails to report information on an adverse action required to be reported under the health care fraud and abuse data collection program established under HIPAA 42 U.S.C. § 1320a-7e(b).

I. Patient Protection and Affordable Care Act

The Patient Protection and Affordable Care Act and the Health Care and Education Reconciliation Act are known collectively as the Affordable Care Act ("ACA"). This law involves broad-ranging reform of the health insurance industry as well as many of the legal authorities addressed above. ACA implements numerous new statutory and regulatory requirements for health insurers, modifies some of the other enforcement authorities discussed herein, and places additional emphasis on governmental enforcement efforts.

J. U.S. Foreign Corrupt Practices Act

The United States' main international anti-bribery law, the U.S. Foreign Corrupt Practices Act ("FCPA"), prohibits providing, directly or indirectly, anything of value to a foreign government official in order to obtain or retain business or otherwise gain a commercial benefit. Foreign government officials may include officeholders, employees of state owned/operated enterprises (*e.g.,* doctors, technicians, employees at a public hospital), military officials, royal family members, or representatives of international organizations (*e.g.*, United Nations or World Bank). The FCPA also imposes record keeping and internal accounting and control requirements to ensure integrity and accuracy in the recording and reporting of all business transactions.

The FCPA is both a criminal and civil statute (enforced by the Department of Justice and Securities and Exchange Commission respectively) and it applies to both entities and individuals. The potential sanctions for FCPA violations can be severe. For violations of the anti-bribery provisions of the FCPA the criminal penalties for individuals are up to $250,00 and/or 5 years imprisonment per violation and for entities up to $2 million per violation. Civil penalties for anti-bribery violations are up to $23,011 per violation for both individuals and entities. Entities may also have to disgorge ill-gotten gains in connection with a bribe and may also be debarred or suspended from participating in multilateral development banks (*e.g.*, World Bank) or federal government procurement programs. For violations of the accounting/controls and record keeping provisions of the FCPA, the criminal penalties for individuals can be up to $5 million and/or 20 years imprisonment per violation and for entities can be up to $25 million per violation. Civil penalties for accounting/controls and record keeping violations for individuals range from $10,360 to $207,183 per violation and for entities from $103,591 to $1,035,909 per violation.

K. General Federal and State Privacy and Data Security Laws

1. Federal Privacy and Data Security Laws:

The United States does not have a comprehensive federal privacy or data security law. However, the Federal Trade Commission (FTC) enforces certain privacy and data security obligations, and there are certain sector-specific privacy and data security laws, like HIPAA (discussed above). The FTC is discussed briefly below, but there are other federal privacy and data security laws that may apply to a given situation.

The FTC's position on privacy and data security is that businesses should use best practices to protect consumer's personal information. The FTC advises businesses to: (1) build privacy into every stage of a business' operations (privacy by design), including reasonable data security, data minimization, reasonable data retention and disposal practices, and the correction and accuracy of data; (2) provide consumers with the ability to make decisions about their personal information; and (3) provide greater transparency relating to the business' collection and use of data, including shorter, clearer, and more standardized privacy notices.

The FTC enforces its privacy and data security guidance through the scope of its authority under Section 5 of the FTC Act, 15 U.S.C. Sec. 45(a)(1), which allows the FTC to investigate and take action against unfair or deceptive business practices. The FTC considers inaccurate privacy notices to be deceptive business practices and data security practices that are not reasonable to be unfair business practices. In addition, the FTC has stated that a failure to notify affected individuals following a data breach may be an unfair or deceptive business practice. To enforce Section 5, the FTC can bring an administrative action against a business. Typically businesses settle with the FTC, and the settlement imposes strict privacy and data security obligations on a business for 20 years. If the business violates the terms of the settlement, the FTC can impose civil monetary penalties which may be as high as ~$43,000 per violation.

2. State Laws:

Like the FTC, state regulators can investigate privacy and data security practices under each state's unfair and deceptive acts and practices laws. They also have other laws that protect personal information, including those in the five states listed below. Other states have other, more comprehensive privacy and data security laws.

Illinois: Violation of Illinois' unfair and deceptive acts and practices law may result in a civil penalty of up to $50,000 (and if a court finds an intent to defraud, a civil penalty of up to $50,000 per violation). 815 Ill. Comp. Stat. 505/1 *et seq*. Pursuant to and subject to the penalties of the foregoing law, businesses or persons that maintain or store personal information of Illinois residents must implement and maintain reasonable security measures, dispose of materials containing personal information in a manner that renders the personal information unreadable, unusable, and undecipherable, and have contractual provisions regarding data security with any third party to whom they disclose Illinois personal information. *Id.* Illinois also has a data breach notification law. If required notice of a data breach is not made, the business is subject to a civil penalty of up to $100 per individual (not to exceed $50,000 per breach). 815 Ill. Comp. Stat. 530/1 *et seq*.

Montana: Willful violation of Montana's Unfair Trade Practices and Consumer Protection Act may result in civil penalties of up to $10,000 per violation. Mont. Code Ann. § 30-14-101 *et seq*. If a business or person violates an order issued relating to an unlawful method, act, or practice, this may result in an additional civil penalty of up to $10,000 for each violation. *Id.* There may also be a criminal penalty of up to $5,000 and imprisonment. *Id*. Montana also has a data breach notification law. If required notice of a data breach is not made, the business is subject to a civil penalty of up to $10,000 per violation. Mont. Code Ann. § 30-14-1701 *et seq*.

New Mexico: Violation of New Mexico's Unfair Practices Act may result in civil penalties of up to $5,000 per violation. N.M. Stat. Ann. § 57-12-1 *et seq*. Also, if a business or person violates New Mexico's data breach notification law knowingly or recklessly, which includes a requirement to implement and maintain reasonable security procedures to protect personal information, the civil penalty may be the greater of $25,000, or in the case of failed notification, $10 per failed notification, not to exceed $150,000. N.M. Stat. Ann. § 57-12C-1 *et seq*.

Oklahoma: Violation of Oklahoma's Consumer Protection Act may result in civil penalties of up to $10,000 per violation and additional penalties may be imposed by a court. Okla. Stat. tit. 15, § 751 *et seq*. Also, a person may be criminally charged with a misdemeanor under the act, including a criminal fine not to exceed $1,000and if the value of the money or property at issue is more than $500 or the person is convicted of a subsequent violation of the act, that person may be charged with a felony and receive a criminal fine not to exceed $5,000. *Id*. Oklahoma also has a data breach notification law. If required notice of a data breach is not made, the business is subject to a civil penalty of up to $150,000 per breach. Okla. Stat. tit. 24, § 161 *et seq*.

Texas: Violation of Texas' Deceptive Trade Practices-Consumer Protection Act may result in civil penalties of up to $10,000 per violation. Tex. Bus. & Com. Code Ann. § 17.01 *et seq*. Further, if a business or person violates Texas' Identity Theft Enforcement and Protection Act, which includes Texas' data breach notification law and a requirement to maintain and update reasonable procedures to protect personal information, there is a civil penalty with a range of $2,000 to $50,000, per violation. Tex. Bus. & Com. Code Ann. § 521.01 *et seq*. Also, in the event of a data breach, if a business or person fails to notify affected individuals, there may be a civil penalty of up to $100 per individual, not to exceed $250,000 per single breach. *Id.* Texas also has a law that limits the use of and protects Social Security numbers. Tex. Bus. & Com. Code Ann. § 501.001 *et seq*. Violations may result in a government investigation and a civil penalty of up to $500 per violation. *Id*. Texas also has the Texas Medical Records Privacy Act, which is a mini-HIPAA. Tex. Health & Saf. Code Ann. § 181.001 *et seq*.

* * *

In short, our organization can never benefit as a result of any employee's misconduct. Our very mission of service can be threatened as a result of an employee's criminal acts.

DM_US 162623566-1.068064.0122