CITY MD
WALK-IN URGENT CARE

Corporate Compliance Program
Code of Ethics and Business Conduct

CITY MD
WALK-IN URGENT CARE
A PARTNER OF
CHI Franciscan Health
# TABLE OF CONTENTS

Introduction  
Part I. Mission and Values  
Part II. Code of Conduct  
1. Overview  
2. Billing & Coding  
3. General Business Practices  
4. Proper Use of CityMD’s Assets  
5. Purchasing Policy  
6. Trade Practices/Antitrust  
7. Compliance with Anti-Kickback Laws  
8. Gifts  
9. Marketing Activities and Patient Referrals  
10. Environment, Health and Safety  
11. Pharmaceuticals, Prescription Drugs, Controlled Substances  
12. HIPAA/Confidential Information  
   - Safeguard the Privacy of Our Patients  
   - Confidentiality of Corporate Information  
   - Information Owned by Others  
   - Records Retention/Destruction  
13. Government Investigations  
14. Human Resources  
Part III. Compliance Procedures  
1. Reporting and Compliant Procedures  
2. Discipline for Violations of the Code of Conduct  
3. Training  
4. Ongoing Compliance Procedures  
5. Annual Report  
Part IV. Individual Judgement  
Conclusion  

Appendix 1  
Appendix 2  
Appendix 2a
Introduction

This Corporate Compliance Plan and Code of Ethics and Business Conduct (the “Compliance Plan”) sets forth standards of conduct that all personnel employed by or associated with City Medical of Upper East Side, PLLC, City Practice Group of New York, LLC, City Medical of New Jersey, PC, City Practice Group of New Jersey, LLC, Franciscan City Urgent Care Services PS, City Management of Washington, LLC, Franciscan City Management, LLC and their related entities and business associates, (“CityMD”) are expected to follow. The Compliance Plan is designed to be a guide and resource to help all personnel ensure that their behavior is in compliance with all laws and regulations that affect all of their business dealings. The Compliance Plan also describes the procedures that will be followed in enforcing these standards and ensuring that CityMD stays in compliance with all applicable laws.

The standards of conduct set forth in the Compliance Plan often exceed those required by law. This is consistent with our commitment to uphold the highest standards of ethical conduct. The standards of conduct, however, cannot cover every situation that our personnel might face. If you are unsure of what a proper course of conduct might be in a specific situation, or believe that the standards of conduct set forth in this Compliance Plan may have been violated, then you are urged to contact CityMD’s “Compliance Officer,” Vincent Campasano, MD at compliance@citymd.net
Part I. Mission and Values

CityMD is committed not only to providing patients with high quality and caring medical services, but also to providing those services faster, better, easier and pursuant to the highest ethical, business, and legal standards. These high standards must apply to our interactions with everyone with whom we deal. This includes our patients, the community, other healthcare providers, companies with whom we do business, government entities to whom we report, and the public and private entities from whom reimbursement for services is sought and received by CityMD. In this regard, all personnel must not only act in compliance with all applicable legal rules and regulations, but also must strive to avoid even the appearance of impropriety. While the legal rules are very important, we must hold ourselves up to even higher ethical standards.

In short, we do not and will not tolerate any form of unlawful or unethical behavior by anyone associated with CityMD. We expect and require all personnel to be law-abiding, honest, trustworthy, and fair in all of their business dealings. To ensure that these expectations are met, the Compliance Plan is an integral part of our corporate culture and business operations.

First and foremost, it is essential that we ensure that we are operating pursuant to the highest ethical standards and in conformity with all applicable legal rules. This is not only the right thing to do, but is also important for our continuing reputation for honesty and integrity in all of our business and medical dealings with others. That reputation has been achieved and maintained through the integrity of our officers and employees, and it is one of our greatest assets; our success depends in large measure upon the trust patients, government regulators, and the public place in us. Our Compliance Plan will help ensure that we live up to this reputation and continue to deserve that trust.

The Compliance Plan must be effective and must be a real part of our culture, mission, and values. CityMD must demonstrate that it is both committed to, and actually exercises, due diligence in seeking to prevent and detect violations of law. To be considered effective, the Federal Sentencing Guidelines require that: (i) the program must establish clear standards; (ii) the program must be administered by a designated Compliance Officer; (iii) all positions involving significant discretionary decision making must be filled by honest employees; (iv) there must be periodic employee training; (v) there must be continuous monitoring of the institution’s business systems; (vi) the program must provide for an enforcement mechanism to deal with violations of the established standards; and (vii) the institutions must respond effectively to such violations.

Because of the importance of the Compliance Plan, we require that each employee cooperate fully. The Compliance Plan will work effectively only if everyone works together to ensure its success, understands what is required under the law and our own Code of Conduct, and works to ensure that those standards are being followed in all of our business dealings. Failure to comply with the standards of conduct set forth in this Compliance Plan can result in serious consequences both to the employee, such as being disciplined, being fired, or even being charged with a crime, and to CityMD, such as criminal prosecution, substantial monetary fines and, of primary importance, the loss of our reputation for honesty and integrity.
Part II. Code of Conduct

This Code of Conduct sets forth the standards of conduct that all personnel are expected to follow. Everyone should adhere both to the spirit and the language of the Code, maintain a high level of integrity in their business conduct and avoid any conduct that could reasonably be expected to reflect adversely upon the integrity or reputation of CityMD.

1. Overview

All personnel associated with CityMD, including physicians, and licensed professionals who may treat patients at our practice sites, must avoid illegal conduct, both in business and personal matters. No personnel will take any action that he or she believes is in violation of any law, rule, or regulation. In addition, all personnel must strive to avoid even the appearance of impropriety, and must never act in a dishonest or misleading manner when dealing with others, both within and outside CityMD.
2. Billing & Coding

CityMD is committed to providing only those medical services to patients that are reasonable and necessary for the diagnosis and treatment of a patient’s illness. Anything more amounts to medically unnecessary “over-utilization” and results in inflated billing to the patient, and to private and governmental third-party payors. While CityMD is committed to providing our patients with the highest quality medical services available, we are also committed to providing, and billing, only those services that are truly appropriate to the patient’s treatment and diagnosis.

To reduce the prospect of erroneous claims and fraudulent activity CityMD has identified the following potential risk areas:

Coding and Billing.

CityMD has identified the following coding and billing risk areas to be monitored:
- Billing for items or services not rendered or not provided as claimed;
- Submitting claims for equipment, medical supplies and services that are not reasonably necessary;
- Double billing resulting in duplicate payment or billing separately for services that are included within the CityMD global rate;
- Billing for non-covered services as if covered;
- Knowing misuse of provider identification numbers, which results in improper billing;
- Unbundling (billing for each component of the service instead of billing or using an all-inclusive code);
- Failure to properly use coding modifiers;
- Failure to correctly identify services ordered;
- Upcoding the level of service provided.

a. Medical Necessity and Quality of Care. CityMD has identified medical necessity as a potential risk area and will take all reasonable measures to ensure that patients are treated in accordance with CityMD’s reasonable evaluation of the patient’s condition and with the goal of providing patients with the highest level of quality of care. In requesting diagnostic procedures or tests, CityMD will make independent medical necessity decisions with regard to each item ordered and will only order tests or services believed to be appropriate for treatment of the patient. A diagnosis will be submitted for all tests ordered and all findings and diagnoses will be documented.

b. Payment. Overpayments or underpayments received from third party payors are an area of potential risk CityMD has identified. In connection with CityMD’s review of coding and billing, CityMD routinely reviews payment remitted to CityMD to ensure compensation reflects services rendered and makes timely refunds to payors as appropriate.

c. Documentation. CityMD has identified the following documentation risk areas to be monitored:
- The medical record is accurate, complete, timely and legible;
- The documentation of each patient encounter includes the reason for the encounter,
any relevant history, physical examination findings, prior diagnostic test results, assessment, clinical impression, or diagnosis, plan of care, and date;
- The clinical rationale for ordering diagnostic and other ancillary services can be easily inferred by an independent reviewer or third party who has appropriate medical training;
- CPT and ICD codes used for claims submission are supported by documentation and the medical record;
- Modifiers are used appropriately;
- All accounts payable must be accompanied by the proper documentation justifying the claim, (electronic or otherwise, contract/invoice), before the payment may be processed.

Physicians, in particular, must comply not only with quality of care standards, but with standards of care for billing as well. In this regard, CityMD's billing procedures must always be based on adequate documentation of the medical justification for the services rendered or test conducted and for the bill submitted, and this medical documentation must comport with all applicable regulations. In addition, all documentation, must also be sufficient to satisfy CityMD's own internal standards for quality assurance as to the services rendered. All federal and state regulations governing billing procedures will be followed, and all personnel responsible for billing and coding will be trained in the appropriate rules governing billing, coding, and documentation. CityMD billing staff also must follow the detailed billing policies and procedures developed within each area of the Billing Department.

Finally, all billing must be accurate and truthful. No personnel should ever misrepresent charges to, or on behalf of, a patient or third-party payor. CityMD bills only for those services that were actually and appropriately rendered. We will not tolerate false statements by any personnel to a government agency or other payor. Deliberate misstatements to government agencies or other payors will expose the personnel involved to criminal penalties and termination.

3. General Business Practices

CityMD will forego any business transaction or opportunity that can only be obtained by improper and illegal means, and will not make any unethical or illegal payments to anyone to induce the use of our services. In the course of CityMD’s business practices, personnel must deal with a variety of individuals, companies, organizations, and governmental agencies. In those dealings, all personnel must never make any misrepresentations, dishonest statements, or statements intended to mislead or misinform. If it appears that anything you have said has been misunderstood, you should correct it promptly.

In addition, management must ensure that all of CityMD’s business records are accurate and truthful, with no material omissions; that the assets and liabilities of CityMD are accounted for properly in compliance with all tax and financial reporting requirements, and that no false records are made. Similarly, all reports submitted to governmental agencies, insurance carriers, or other entities will be accurately and honestly made.

4. Proper Use of CityMD’s Assets

All managers should establish appropriate internal accounting controls over all areas of their responsibility to ensure the safeguarding of CityMD’s assets and the accuracy of financial records and reports. These established accounting practices and procedures must be followed to assure the complete and accurate recording of all transactions. CityMD has
adopted these controls in accordance with the Generally Accepted Accounting Principles ("GAAP"), internal needs and the requirements of other applicable laws and regulations. All employees, within their areas of responsibility, are expected to adhere to these established controls.

If you become aware of any improper use of, or accounting practice inconsistent with, GAAP concerning CityMD's resources, you should report the matter immediately to the Corporate Compliance Officer at compliance@citymd.net or to the General Counsel, (212) 913-0828 extension 1063. To be certain CityMD’s policies on proper use of resources are carried out, you are expected to observe the following longstanding accounting rules:

- Make outside payments only with a draft or check or through other properly documented sources. No payment on behalf of CityMD should be approved or made without adequate supporting documentation or with the intention or understanding that any part is to be used in any way other than described in the supporting documents;
- Do not establish any undisclosed or unrecorded corporate account, fund or asset for any purpose;
- Get proper authorization before opening any new account, either on CityMD’s books or with an outside agency, such as a bank;
- Do not use any account for a misleading purpose or to conceal the existence or use of any corporate resource;
- Record every payment to and every transaction with an outside party on CityMD’s books promptly, accurately and through normal financial reporting channels. If you are involved in or accountable for any such transaction, you are expected to make sure a prompt and accurate accounting is made.

You are also expected to select CityMD’s business partners solely on their merits, in the best interest of CityMD, and without regard to non-business related considerations. The following is an example of the kind of relationship with a business partner that is:

- Personal financial involvement or ownership of a substantial interest that has not been disclosed and approved in accordance with CityMD’s Conflict of Interest Policy in organizations with whom CityMD does business, such as vendors, suppliers, agents, customers, contractors, licensees or sponsors. Anything that would constitute improper or questionable behavior on the part of an employee is also unacceptable if engaged in through a third party, such as a spouse, other family member, friend or any other person or entity with whom the employee is closely identified or in which he or she has any significant ownership or financial interest or position.

5. Purchasing Policy

All purchasing decisions must be made with the purpose of obtaining the highest quality product or service for CityMD or its patients at the most reasonable price. No purchasing decision may be made based on any consideration that any employee, officer or partner - or any family member or friend of any of them — will benefit by the transaction. Rather, the sole criteria behind all purchasing decisions must be only the best interests of CityMD. Nor can any service or item be purchased in return for a referral of patients from another or with a view towards inducing another to refer patients (see also the rules governing Marketing Activities and Patient Referrals set forth below in Section 9).
6. Trade Practices/Antitrust

Antitrust laws are designed to preserve and foster fair and honest competition within the free enterprise system. To accomplish this goal, the language of these laws is deliberately broad, prohibiting such activities as “unfair methods of competition” and agreements “in restraint of trade”. Such language gives enforcement agencies the right to examine many different business activities to judge the effect on competition.

CityMD’s policy requires full compliance with all antitrust laws. No employee, under any circumstances, has the authority to approve a violation of the law. Anyone who violates the law or knowingly permits a subordinate to do so is subject to disciplinary action, including dismissal. Penalties for antitrust violations are severe for CityMD and the individual. They include:

- Imprisonment;
- Substantial fines against CityMD and the individual for each criminal offense. Payment of treble damages, plus attorneys’ fees and litigation costs, to firms or individuals injured by the violation;
- Injunctions or consent decrees prohibiting certain activities. Consent decrees can seriously limit a company’s future freedom to engage in business activity and can be applied across a broader scope than was involved in the original alleged violation.

It is important that you have a basic knowledge and understanding of the requirements of antitrust laws. The greatest danger for violations of antitrust laws rests in contacts with competitors. Antitrust laws make illegal any agreement or understanding, expressed or implied, written or oral, which restricts competition or interferes with the ability of the free market system to function properly. In the eyes of the law, good intentions, customer benefits or consumer benefits do not justify or excuse violations. For CityMD, a “competitor” may be another hospital or any other healthcare provider.

You should not have any discussions, conversations or other communications with competitors about the division of either patients, geographic areas, or services; the circumstances under which business will be conducted with suppliers, insurance companies, patients or customers; or marketing efforts. Further, you should avoid discussions with competitors regarding the future business plans of CityMD or any competitors. Finally, you should not have any discussions with competitors regarding prices or reimbursement or salary levels. If you have questions, contact the Legal Department.

7. Compliance with Anti-Kickback Laws

Both federal and state laws specifically prohibit any form of kickback, bribe or rebate made directly or indirectly, overtly or covertly, in cash or in kind to induce the purchase, recommendation to purchase or referral of any kind of healthcare goods, services or items paid for by Medicare or the Medicaid program. The term “kickback” as defined in these laws
means the giving of anything of value in exchange for patient referrals. Under the federal law, the offense is classified as a felony and is punishable by fines and imprisonment. Federal and state "anti-referral" laws impose substantial penalties relative to billing for services referred by physicians or other healthcare practitioners who have a contractual or business relationship with CityMD. You should become familiar with these laws and assure that all of your activities are conducted in such a manner that no question may arise as to whether any of these laws have been violated. Any question concerning these laws or any business arrangement subject to anti-kickback or anti-referral laws should be directed to the General Counsel.

To list everything that may constitute an improper inducement under the anti-kickback laws would not be possible. However, CityMD must scrupulously avoid being either the offeror or the recipient of an improper inducement. Care must be taken in structuring relationships with persons not employed by CityMD so as not to create a situation where CityMD appears to be offering an improper inducement to those who may be in a position to refer or influence the referral of patients to CityMD. For example, the offering of free goods or services, or those priced below market value, to physicians for the purpose of influencing them to refer patients to, or utilize the professional services offered by, CityMD would be improper.

CityMD has identified the following risk areas to monitor:

- Financial arrangements with outside entities to whom CityMD may refer patients of from which CityMD receives referrals;
- Joint ventures with entities supplying goods or services to CityMD or its patients;
- Consulting contractors or medical directorships;
- Waiver of coinsurance or deductible amounts, in a manner not consistent with CityMD policy;
- Soliciting, accepting or offering any gift or gratuity of more than nominal value to or from those who may benefit from a CityMD referral.

As a provider of patient care, CityMD also should not receive any improper inducement from its vendors to influence it in making decisions regarding the use of particular products or the referral or recommendation of patients to other providers of goods and services. For example, free, or at below-market value, goods or services from vendors, awards, discounts, prizes or other forms of remuneration may be treated as a "kickback" even if given as part of a promotional program of a vendor or provider, e.g., pharmaceutical company, medical equipment supplier, etc. There are certain exceptions to these rules which permit discounts, rebates and allowances under appropriate circumstances, provided there is proper disclosure of the discount or other remuneration to third-party payers.

Before entering into any business or contractual relationship with any person or organization which may raise a question under the anti-kickback laws, or with any physician or other healthcare practitioner who makes or may make referral to CityMD, please consult with the Legal Department. All contracts must be reviewed by the Legal Department prior to execution.

Likewise, it is a violation of CityMD's policy, and an offense for which dismissal will be considered, for any officer, employee or any other person acting on behalf of or in the name of CityMD to make or authorize the paying of any bribe, any payment for an illegal act or any other use of a CityMD resource which, although arguably not illegal, could be interpreted as
improper or unwarranted.

In general, any money, property or favor offered or given to induce someone to forego
normal business or professional considerations in making decisions that affect CityMD
constitutes improper use of a resource. Equally improper is any payment of any kind to
consultants, agents, brokers, attorneys, other individuals or firms if there is reason to suspect
that some or all of the payment is to be used to do anything that is prohibited by this Code.

A useful test to apply in determining whether a payment - or any other transaction - is
proper is whether such transaction, if disclosed publicly, could adversely affect the reputation of
CityMD. Another useful principle to follow is not to give anything to a vendor, client or other
person doing business with CityMD which you could not yourself accept under CityMD’s
policies (see Gifts and Entertainment) if it were offered to you under similar circumstances. If
you have any doubts as to whether a payment is lawful, you should consult your manager,
the Compliance Officer, or our Legal Department.

8. Gifts

No personnel will engage, either directly or indirectly, in any corrupt business practice,
including bribery, kickbacks or payoffs, intended to influence or reward favorable decisions of
any patient, physician, government representative, contractor, or vendor in a commercial
transaction, or any other person in a position to benefit CityMD or the employee in any way.
No employee will make or offer to make any payment or provide any other thing of value to
another person with the understanding or intention that such payment is to be used for an
unlawful or improper purpose.

Gifts cannot be given or received for the purpose of influencing the business behavior of
the recipient. Cash gifts are strictly prohibited. Non-cash gifts made to CityMD staff members or
owners from individuals who seek to obtain our patient referrals are also strictly prohibited.
Gifts of even nominal value may not be offered to any governmental official. Such gifts can
be misinterpreted as an attempt to improperly influence the official and are to be avoided.
Any questions regarding whether or not an item or situation falls within the scope of this
section must be raised immediately with the Legal Department of CityMD.

9. Marketing Activities and Patient Referrals

CityMD is committed to the delivery of high quality medical care, and relies on the
quality of that care in marketing its services to patients, physicians, and other healthcare
providers who might refer patients. All marketing activities and advertising by personnel must
be truthful and not misleading and must be consistent with New York, New Jersey and
Washington State regulations on physician practice advertising, and must be supported by
evidence to substantiate any claims made. CityMD’s best advertisements are the quality of
the medical services we provide. No personnel should disparage the service or business of a
competitor through the use of false or misleading representations.

CityMD does not pay incentives to any employee based upon the number of
persons referred for treatment or the value of services provided. The decision to refer patients
is a separate and independent clinical decision made by the referring physician or healthcare
provider. Nor does CityMD pay physicians, or anyone else, either directly or indirectly, for
patient referrals. Federal and state law makes it unlawful to pay any individual on the basis of
the value or volume of referral of patients. This includes the giving of any form of remuneration,
including virtually anything of value, in return for a referral. Conversely, CityMD does not
accept any form of remuneration in return for referring our patients to other healthcare providers.

10. Environment, Health and Safety

In the course of CityMD’s operations, hazardous materials and infectious wastes may be used or generated. CityMD is financially and legally responsible for the proper handling and disposal of these materials. Environmental responsibility is also an important component of our duty to the public and our good reputation. It is essential that everyone at CityMD who deals with hazardous materials and infectious waste complies with environmental laws and regulations, and follows the environmental safety procedures explained in CityMD’s programs and existing manuals. Employees are also expected to enable CityMD to:

- Comply with all laws and regulations governing the handling, storage and use of hazardous materials, other pollutants and infectious wastes;
- Comply with its permits that allow it to safely discharge pollutants into the air, sewage systems, water pollution control facilities, or onto/into land;
- Hire only reputable licensed services to transport and dispose of hazardous and polluted materials and infectious wastes;
- Accurately maintain the records required by the environmental laws and regulations, including those that require precise description of the amount, concentration and make-up of hazardous materials or other regulated pollutants and infectious wastes that are used, stored, discharged or generated; and the time, place of origin, destination and transporter of hazardous materials, and discharge of pollutants. These records should be handled pursuant to proper CityMD policy.

No one at CityMD may participate in concealing improper discharge or disposal of hazardous materials, pollutants or infectious wastes. Any employee who has reason to believe that there have been violations of this or any other aspect of CityMD’s environmental compliance procedures should report immediately to the Compliance Officer, who will investigate and, when appropriate, notify pertinent government agencies as required by law. Before proceeding to act on any instruction of questionable propriety, or to take any environment-related action about which they are unsure, employees are expected to discuss their questions with the General Counsel.

11. Pharmaceuticals, Prescription Drugs, Controlled Substances

Many of CityMD’s employees have responsibility for or access to prescription drugs, controlled substances, hypodermic needles, drug samples and other regulated pharmaceuticals. CityMD is legally responsible for the proper distribution and handling of these pharmaceutical products. Federal, state and local laws covering prescription drugs and controlled substances are intended to maintain the integrity of our national drug distribution system and protect consumers by assuring that prescription drugs are safe and properly labeled.

These laws include prohibitions against diversion of any prescription drug or controlled substance, including a drug sample, in any amount for any reason to an unauthorized individual or entity. The distribution of adulterated, misbranded, mislabeled, expired or diverted pharmaceuticals is a violation of federal and state law for which severe criminal penalties may be imposed on individual violators as well as on CityMD.
It is CityMD’s policy that all employees be both diligent and vigilant in carrying out their obligations to handle and dispense CityMD’s prescription drugs and controlled substances in accordance with all applicable laws, regulations and CityMD procedures. These CityMD procedures and policies are available in written form from the Legal Department of Medical Control.

Every professional employee, whether physician, or any other licensed individual authorized to prescribe, dispense, or handle prescription drugs or controlled substances, is expected to maintain the highest professional standards in safeguarding pharmaceuticals of all kinds and in preventing unauthorized access to them. This includes adherence to laws and regulations governing procedures for securing scheduled controlled substances and for their return or destruction.

No prescription drug or controlled substance may be sold, transferred or otherwise distributed unless authorized by a written Practice policy or the appropriate Practice individual charged with such responsibility. Any violation of any law or of any Practice policy involving prescription drugs, controlled substances or other pharmaceuticals will constitute grounds for dismissal. Each employee is expected to protect the integrity of CityMD by safeguarding the drugs entrusted to us for appropriate institutional medical use. If you become aware of any potential lapses in security, or any actual infringement of any law, policy or regulation relating to drugs, you must advise your manager or The Compliance Officer immediately.

All physicians and physician assistants must adhere to CityMD’s policies regarding the review of applicable electronic prescription monitoring databases prior to issuing a prescription for a controlled substance.

12. HIPAA and Other Confidential or Protected Information

The Health Insurance Portability and Accountability Act (“HIPAA”) provides federal protections for personal health information (PHI) held by CityMD and provides patients an array of rights with respect to that information. At the same time, the law is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes. The HIPAA Security Rule specifies a series of administrative, physical, and technical safeguards for CityMD to assure the confidentiality, integrity, and availability of electronic protected health information.

Safeguard the Privacy of our Patients

To ensure compliance not only with HIPAA, but with New York, New Jersey and Washington State rules regarding the confidentiality of patient information, CityMD has developed a number of specific HIPAA policies. These policies are available on the CityMD internal web site (wearcitymd.com). All staff members are required to be familiar with and abide by the CityMD HIPAA policies. Any questions or concerns about the use or disclosure of patient information should be directed to our HIPAA Privacy Officer; Blair Durst, Esq., (212) 913-0828 extension 1004.

Confidentiality of Corporate Information

Confidential information acquired by personnel about the business of CityMD must be held in confidence and may not be used as a basis for personal gain by the personnel, their families, or others. Information relating to transactions pending with CityMD is not to be
released to any person unless this information has been published or otherwise made generally available to the public. Similarly, if CityMD is considering buying, leasing, or selling any property, item, or interest, CityMD employees and affiliates must not attempt to buy, lease, or sell for their own benefit or that of their family the item under consideration, until CityMD's decision on the matter has been executed. Finally, other than in connection with the employee's discharge of their official responsibilities with CityMD, all personnel must also refrain from disclosing information about CityMD consideration or decision, or any other information which might be prejudicial to the interest of CityMD.

The governing principle is that if any material confidential information pertaining to CityMD is received by personnel, they must not use such information for their own or their family's benefit, nor should they disclose it to others for their personal use.

*Information Owned by Others*

Like CityMD, other organizations have intellectual property they want to protect. So do individuals. These other parties are sometimes willing to disclose their confidential information for a particular purpose. If you are on the receiving end of another party's confidential information, you must proceed with caution to prevent any accusations that you or CityMD misappropriated or misused the information.

To avoid the risk of being accused of misappropriating or misusing someone’s confidential or restricted information, there are certain steps you should take before receiving such information. The receipt of confidential or restricted information whether oral, visual or written must not take place until the terms of its use have been formally agreed to by CityMD and the other party. That means a written agreement, Non-Disclosure Agreement or Confidentiality Agreement approved by the General Counsel. Furthermore, unless otherwise delegated, establishing such an agreement for the receipt of confidential or restricted information of another party will require the prior written approval of an appropriate Practice Officer. Once another party’s confidential or restricted information is properly in your hands, you must not use, copy, distribute or disclose that information unless you do so in accordance with the terms of the agreement.

Special care should be taken in acquiring software from others. As intellectual property, software is protected by copyright laws and may also be protected by patent, trade secret laws or as confidential information. Such software includes computer programs, databases and related documentation owned by the party with whom you are dealing or by another party. Before you accept software or sign a license agreement, you must follow established CityMD procedures. The agreement must be reviewed and approved by the General Counsel. The terms and conditions of such license agreements - such as provisions not to copy or distribute programs - must be strictly followed. Also, if you acquire software for your personally-owned equipment, you should not copy any part of such software in any work you do for CityMD, place such software on any CityMD-owned computer system, or generally bring such software onto CityMD premises. In any case, do not take the status of information for granted. If you have information in your possession that you believe may be confidential to a third party or may have restrictions placed on its use, you should consult with the General Counsel.

*Records Retention/Destruction*

CityMD is required by law to maintain certain types of medical and business records, usually for a specified period of time. Failure to retain such documents for such
minimum period could subject CityMD to penalties and fines, cause the loss of rights, obstruct justice, place CityMD in contempt of court or put CityMD at a serious disadvantage in litigation. Accordingly, CityMD has written policies regarding the retention/Destruction of documents to assure retention for required periods and timely destruction of retrievable records, such as hard copies and records on computers, electronic systems, microfiche and microfilm. Even if a document is retained for the minimum period, legal liability could still result if a document is destroyed before its scheduled destruction date.

You are expected to comply fully with the records retention and destruction schedule for the department in which you work. If you believe that documents should be saved beyond the applicable retention period, consult your manager, who in turn should contact the Legal Department.

It is likewise critical to the successful accomplishment of CityMD’s professional goals that its records be fully and accurately completed and maintained consistent with proper business practices. Many of CityMD records serve as a basis for treatment decisions for its patients, as a compilation of goods and services rendered for billing purposes and as a recordation of historical courses of treatment. Each of these functions serves an indispensable role in enabling CityMD to fulfill its obligations to its patients, the medical and nursing staff and the various payors for goods and services. Consequently, the proper and contemporaneous creation of fully accurate and complete records is a duty of each member of CityMD.

13. Government investigations

Given the increased vigilance by law enforcement agencies in the healthcare arena, it is important that CityMD establish definitive guidelines on how and when to respond to government inquiries. Inaccurate or incomplete information provided to government officials in response to their inquiries will more often than not generate complications for CityMD and possibly frustrate the legitimate purposes of the inquiry. Unauthorized disclosure of information may jeopardize our patient’s rights to privacy and expose the organization to inability. Therefore we must adhere to the following procedures to ensure CityMD responds in a proper manner to all government investigations.

Any personnel who receive a governmental request for information, a subpoena, or any other inquiry or legal document regarding CityMD business must notify the Office of General Counsel immediately.

If a response is given to a request for information from government regulatory agencies, the response must be accurate and complete. It is CityMD’s policy to comply with the law and to cooperate with reasonable demands made during the course of a governmental investigation or inquiry. Any employee of CityMD who is approached by any federal or state law enforcement agency seeking information about any aspect of the operations of CityMD or the job-related activities of any of CityMD’s officers, employees, or agents should contact the Legal Department before turning over any information.

14. Human Resources

CityMD recognizes that its greatest strength lies in the talent and ability of its employees. Accordingly, CityMD has developed and implemented numerous human resources policies and has published for CityMD staff members the Employee Handbook, which is posted on the CityMD internal web site (wearecitymd.com).
Part III. Compliance Procedures

This section of the Compliance Plan summarizes the rules under which the Compliance Plan will operate. To be effective, a Compliance Plan must provide for the following: continued reporting of issues or possible violations of the Code of Conduct to the Compliance Officer and periodic reports by the Compliance Officer to the Board of Directors; enforcement of the Code through the promulgation of disciplinary procedures; continued, periodic reviews and self-audits of our business practices; and implementation of modifications in the Compliance Plan, as necessary, to prevent future violations.

1. Reporting and Complaint Procedures

All personnel should raise any compliance issues as soon as possible. Employees can initially go to their supervisor with compliance concerns that they have. If you are uncomfortable going to your supervisor or the matter is not resolved following your raising it with your supervisor, you can raise your issue with the Corporate Compliance Officer and/or the General Counsel. The failure to report a compliance issue of which you are aware may result in disciplinary action against you or others who fail to report. Moreover, even if you merely have a general question about the propriety of conduct, you should still reach out to the Compliance Officer for guidance. He is the compliance program’s “point person,” to whom all officers and employees can turn to express concerns about such matters.

Your report or question may be raised anonymously, if you choose, and will be held in the strictest confidence possible, consistent with the need to investigate any allegations of wrongdoing. To the extent possible, the Compliance Officer will not disclose the identity of anyone who reports a suspected violation of law or who participates in an investigation. All personnel should be aware, however, that the General Counsel, is obligated to act in the best interests of CityMD and does not act as the personal representative or lawyer for employees. Upon receiving a report of possible unethical or illegal conduct, the Compliance Officer will bring such report, as appropriate, to the attention of senior management, and conduct an investigation. All personnel are expected to cooperate in such investigations.

Retaliation in any form against an individual who in good faith reports possible unethical or illegal conduct is strictly prohibited and is itself a serious violation of the Code of Conduct. Acts of retaliation should be reported to the Compliance Officer immediately.

The Compliance Officer will maintain a written record of all reports made of suspected wrongdoing; of all steps taken to investigate those reports; and of all determinations made as a result of any investigation that may be undertaken.

2. Discipline for Violations of the Code of Conduct

All personnel are expected to adhere to the Compliance Plan and Code of Conduct. If the Compliance Officer concludes, after an appropriate investigation, that the Code has been violated, then he will recommend appropriate discipline, including discharge. Such recommendation can be based on the employee’s unlawful or unethical actions, condoning or failing to report improper actions by others, retaliation against those who report suspected wrongdoing, or other violations of the Compliance Plan.
3. Training

All staff members are required to participate in compliance training on an annual basis, and also are required to participate in all education and training session to stay proficient in areas that impact their job performance.

4. Ongoing Compliance Procedures

On a regular, periodic basis, the Compliance Officer will ensure that a review is conducted of CityMD’s billing practices. These reviews will include, but are not limited to, such things as the following:

- A review of the reports of suspected violations of the Code of Conduct to determine if there are any patterns in the violations that might indicate broader compliance issues;
- A small random sampling of the medical records and corresponding bills. If these samples uncover substantial billing or documentation errors, then the Compliance Office will broaden the audit, as appropriate, to determine the scope of the problem, if any.

If any of these reviews indicate that possible compliance issues might exist, the Compliance Officer will inform the General Counsel and a determination will then be made whether further investigation is required and whether CityMD’s practices need to be modified or improved in any way to ensure continuing compliance with applicable federal and state laws and regulations.

Finally, should federal or state laws change in any relevant manner, the Legal Department will inform the Compliance Officer and work with CityMD to make any appropriate changes in its business practices, update this Compliance Plan, or conduct additional training.

5. Annual Report

On no less than an annual basis, the Compliance Officer will report to the Board of Directors, and will describe the compliance efforts that have taken place during the prior year and any changes implemented to the Compliance Plan that he recommends be made to improve compliance.

Part IV. Individual Judgment

The foregoing guidelines are to help all of us better understand what we believe to be in the best interest of our employees, patients, those with whom we do business and the public at large. Ultimately, however, you are left to depend on your own individual judgment in deciding on the correct course of action. As you contemplate a particular situation, consideration of the following factors may help you arrive at a satisfactory answer:

- Is my action consistent with CityMD’s practices?
- Could my action give the appearance of impropriety?
- Will the action bring discredit to any employee of CityMD if disclosed fully to the public?
- Can I defend my action to my manager, other employees and to the general public?
• Does my action meet my personal code of behavior?
• Does my action conform to the spirit of this Code of Ethics and Business Conduct?

Remember always to use good judgment and common sense. This Code of Ethics and Business Conduct is intended to reflect the collective good judgment and common sense of all of us. Whenever you see a situation where this purpose does not appear to be served by the Code, you have the responsibility to bring your concerns to the attention of the Compliance Officer.

**Conclusion**

This Code of Ethics and Business Conduct is designed to educate you about some of the laws and regulations that govern CityMD’s practice of medicine and related billing and business issues. It has also been designed to raise your consciousness, by demonstrating the complexity of the myriad laws.

If this Compliance Plan does nothing else, it should motivate you to think seriously about compliance issues and how they impact your professional life and practice. Just as important, it should motivate you to contact the Compliance Officer with any questions or concerns you might have.
EMPLOYEE HOTLINE
compliance@citymd.net
Appendix 1

Code of Ethics and Business Conduct

Fraud and Abuse Laws and Regulations Applicable to Healthcare Businesses

Deficit Reduction Act

As a provider that receives payment through the Medicaid Program, we must comply with the terms of the Deficit Reduction Act of 2005 (the "DRA"). The DRA, specifically Section 6033, entitled "Employee Education About False Claim Recovery," which was effective January 1, 2007, requires any organization that receives $5 million or more in Federal Medicaid funds annually (including payments from managed care companies) to adopt a compliance program in accordance with Federal law and to inform its employees and contractors of the terms of the False Claims Act. Any organization that does not comply with the requirements may be denied Medicaid reimbursement.

False Claims Act

The federal government amended the False Claims Act (FCA) to make it a more effective tool. Using the False Claims Act, private citizens (i.e., whistleblowers) can help reduce fraud against the government. The Act allows everyday people to bring suits against groups or other individuals that are defrauding the government.

For the purposes of this Appendix and the CityMD Code of Ethics and Business Conduct, "knowing and/or knowingly" means that a person, with respect to the information, has actual knowledge of the information; acts in deliberate ignorance of the truth or falsity of the information; or acts in reckless disregard of the truth or falsity of the information. No proof of specific intent to defraud is required.

The federal False Claims Act (FCA) applies when a company or person:

- Knowingly presents (or causes to be presented) to the federal government a false or fraudulent claim for payment
- Knowingly uses (or causes to be used) a false record or statement to get a claim paid by the federal government
- Conspires with others to get a false or fraudulent claim paid by the federal government
- Knowingly uses (or causes to be used) a false record or statement to conceal, avoid, or decrease an obligation to pay or transmit money or property to the federal government
False Claims Act Penalties

Those who defraud the government, can end up paying triple (or more than) the damage done to the government, or a fine for every false claim, in addition to the claimant's costs and attorneys' fees. These monetary fines are in addition to potential incarceration, revocation of licensures, and/or becoming an "excluded" individual, which prevents an individual from being employed in any job that receives monies from the federal government, the state government, or both.

FCA: Whistleblower Protections

The False Claims Act allows everyday people to bring suits against organizations or individuals who are defrauding the government. These individuals are commonly known as "whistleblowers." If the government moves forward with a case, the individual who brings the suit is generally entitled to receive a percentage of any recovered funds once a decision has been made. If the government decides not to pursue the case, then the individual must pursue the issue on his or her own and, if successful, then he or she would be entitled to a percentage of any recovered funds as well.

Federal laws shield employees from retaliation for reporting illegal acts of employers. An employer cannot retaliate in any way, such as discharging, demoting, suspending or harassing the whistleblower. If an employer does retaliate, the employee may be entitled to file a charge with a government agency, sue the employer, or both.

To report information about fraud, waste, or abuse involving Medicare or any other healthcare program involving only federal funds, call the toll-free hotline established by the federal Office of Inspector General in the U.S. Department of Health and Human Service. The hotline number is 1-800-HHS-TIPS (1- 800- 447-8477).

For more information about this hotline and about other ways to contact the Office of Inspector General, you can go to https://oig.hhs.gov/fraud/report-fraud/index.asp.

Stark Law

The Stark Law governs physician self-referral for Medicare and Medicaid patients. Physician self-referral is the practice of a physician referring a patient to a medical facility in which he/she has a financial interest, be it ownership, investment, or a structured compensation arrangement. The law prohibits physicians from referring Medicare patients for certain designated health services to an entity with which the physician, or a member of the physician's immediate family,
has a financial relationship—unless an exception applies. It also prohibits an entity from presenting, or causing to be presented, a bill or claim to anyone for a health service furnished as a result of a prohibited referral.

Violations of the Stark Law and the practice of physician self-referral are to be reported to the Centers for Medicare and Medicaid Services via its self-disclosure process.

**Anti-Kickback Statute**

The federal Anti-kickback law provides for criminal and civil penalties for certain acts which impact Medicare and Medicaid or any other federally funded or State-funded program. If you solicit or receive any remuneration in return for referring an individual to a person (doctor, hospital, and provider) for a service for which payment may be made, it can be seen as a potential kickback. Remuneration includes payment, monies, or any goods or services from any healthcare facilities, programs, or providers.

**Federal Program Fraud Civil Remedies Act**

This act provides federal administrative remedies for false claims and statements, including those made to federally-funded healthcare programs. Civil penalties accrue for each false claim or statement, and an assessment in lieu of damages sustained by the federal government of up to double damages for each false claim for which the government makes a payment.
Appendix 2

Code of Ethics and Business Conduct

CMS Fraud and Abuse Prevention Training PowerPoint
Module 10

Medicare and Medicaid Fraud and Abuse Prevention

Session Objectives

This session should help you

- Define fraud and abuse
- Identify causes of improper payments
- Discuss how CMS fights fraud and abuse
- Explain how you can fight fraud and abuse
- Recognize sources of additional information
Lesson 1—Fraud and Abuse Overview

- Definition of fraud and abuse
- Protecting the Medicare Trust Funds and other public resources
- Examples of Medicare and Medicaid fraud
- Who commits fraud?
- Causes of improper payments
- Quality of care concerns

Definition of Fraud and Abuse

**Fraud**
When someone intentionally executes or attempts to execute a scheme to obtain money or property of any health care benefit program

**Abuse**
When health care providers or suppliers perform actions that directly or indirectly result in unnecessary costs to any health care benefit program

The primary difference between fraud and abuse is intention.
Protecting Taxpayer Dollars

- CMS must
  - Protect Medicare Trust Funds
    - Medicare Hospital Insurance (Part A) Trust Fund
    - Supplementary Medical Insurance (Part B) Trust Fund
  - Protect the public resources that fund the Medicaid programs
  - Manage the careful balance between
    - Paying claims quickly and limiting burden on the provider community with conducting reviews that prevent and detect fraud

Examples of Fraud

- Medicare or Medicaid is billed for
  - Services you never received
  - Equipment you never got or was returned
- Documents are altered to gain a higher payment
- Misrepresentation of dates, descriptions of furnished services, or the identity of the beneficiary
- Someone uses your Medicare or Medicaid card with or without your permission
- A company uses false information to mislead you into joining a Medicare plan

For recent examples of fraud by region visit, medic-outreach.rainmakerssolutions.com/fraud-in-the-news/.
Consequences of Sharing a Medicaid Card or Number

- Medicaid-specific lock-in program
  - Limits you to certain doctors/drug stores/hospitals
    - For activities like ER visits for non-emergency care and using multiple doctors that duplicate treatment/medication
- Your medical records could be wrong
- You may have to pay money back or be fined
- You could be arrested
- You might lose your Medicaid benefits

Who Commits Fraud?

- Most individuals and organizations that work with Medicare and Medicaid are honest
- However, anyone can commit fraud
  - Doctors and health care practitioners
  - Suppliers of durable medical equipment
  - Employees of doctors or suppliers
  - Employees of companies that manage Medicare billing
  - People with Medicare and Medicaid
Improper Payment Transparency

**MEDICARE FY 2013**
Error rate is 10.1 percent or $36 billion

**MEDICAID FY 2013**
Error rate is 5.8 percent or $14.4 billion

Projected Improper Payments for Medicare Fee-for-Service

Fiscal Reporting Year

Projected Improper Payments for Medicaid

Fiscal Reporting Year

5/01/2014

Medicare and Medicaid Fraud and Abuse Prevention

---

Causes of Improper Payments

- Not all improper payments are fraud, but all payments made due to fraud schemes are improper

- CMS is targeting all causes of improper payments
  - From honest mistakes to intentional deception
  - Most common error is insufficient documentation
Preventing Fraud in Medicare Parts C and D

- Plan agents and brokers must follow CMS's Marketing Guidelines. Examples of what plans can’t do include
  - Send you unwanted emails
  - Come to your home uninvited to get you to join
  - Call you unless you’re already a member
  - Offer you cash to join their plan
  - Give you free meals while trying to sell you a plan
  - Talk to you about their plan in areas where you get health care

- If you think a Medicare plan broke the rules
  - Call 1-800-MEDICARE (1-800-633-4227)
  - TTY users should call 1-877-486-2048

Telemarketing and Fraud—Durable Medical Equipment (DME)

- DME telemarketing rules
  - DME suppliers can’t make unsolicited sales calls

- Potential DME scams
  - Calls or visits from people saying they represent Medicare
  - Telephone or door-to-door selling techniques
  - Equipment or service is offered free and you’re then asked for your Medicare number for “record keeping purposes”
  - You’re told that Medicare will pay for the item or service if you provide your Medicare number
Quality of Care Concerns

- Patient quality of care concerns aren’t necessarily fraud
  - Medication errors
  - Change in condition not treated
  - Discharged from the hospital too soon
  - Incomplete discharge instructions and/or arrangements
- Contact your Beneficiary and Family-Centered Care Quality Improvement Organization
  - Visit Medicare.gov/contacts and click on Find Helpful Contacts
  - Call 1-800-MEDICARE (1-800-633-4227)
  - TTY users should call 1-877-486-2048

Check Your Knowledge—Question 1

Those who commit Medicare fraud can include
a. People with Medicare
b. Suppliers of durable medical equipment
c. Doctors and health care practitioners
d. All of the above
Check Your Knowledge—Question 2

It's considered fraud if someone else uses your Medicare card with your permission

a. True
b. False

Lesson 2—CMS Fraud and Abuse Strategies

- The Center for Program Integrity
- CMS Program Integrity Contractors
- CMS Administrative Actions
- Law Enforcement Actions
- The Health Care Fraud Prevention Partnership
- Health Care Fraud Prevention and Enforcement Action (HEAT) Team
- The Fraud Prevention Toolkit at CMS.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/fwa.html
- Provider and Beneficiary Education
CMS Center for Program Integrity

- Consolidates CMS anti-fraud components
- Authorities from the Affordable Care Act
  - More rigorous screenings for health care providers
  - Reciprocal termination of providers from Medicare, Medicaid, and the Children’s Health Insurance Program
  - May temporarily stop enrollment in high-risk areas
    - Used first in July 2013 and extended into 2015
  - Temporarily stop payments in cases of suspected fraud

5/01/2015 Medicare and Medicaid Fraud and Abuse Prevention

CMS Program Integrity Contractors

- A nationally coordinated Medicare/Medicaid program integrity strategy that cuts across regions
  - Zone Program Integrity Contractors (ZPIC)
  - National Benefit Integrity Medicare Drug Integrity Contractor (NBI MEDIC)
  - Recovery Audit Program
  - Outreach & Education MEDIC (O&E MEDIC)
  - Medicaid Integrity Contractors

5/01/2015 Medicare and Medicaid Fraud and Abuse Prevention
**Zone Program Integrity Contractors (ZPICs)**

- Investigate leads generated by the new Fraud Prevention System (FPS) and a variety of other sources
- Provide feedback to CMS to improve the FPS
- Perform data analysis to identify and investigate cases of suspected fraud, waste, and abuse
- Make recommendations to CMS for appropriate administrative actions to protect Medicare Trust Fund dollars
- Make referrals to law enforcement for potential prosecution
- Provide support for ongoing law enforcement investigations
- Identify improper payments to be recovered by Medicare Administrative Contractors
National Benefit Integrity Medicare Drug Integrity Contractor (NBI MEDIC)

- Monitors fraud, waste, and abuse in the Part C and Part D programs in all 50 states, the District of Columbia, and U.S. Territories
- Works with law enforcement and other stakeholders
- Key responsibilities include
  - Investigate potential fraud, waste, and abuse
  - Receive complaints
  - Resolve beneficiary fraud complaints
  - Perform proactive data analyses
  - Identify program vulnerabilities
  - Refer potential fraud cases to law enforcement agencies
- The Outreach and Education MEDIC provides tools to combat Part C and Part D fraud, waste and abuse

5/01/2015
Medicare and Medicaid Fraud and Abuse Prevention

Recovery Audit Program

- Recovery Audit Program's mission
  - Reduce improper Medicare payments by
    - Detecting and collecting overpayments
    - Identifying underpayments
    - Implementing actions to prevent future improper payments
  - Ensure that each Medicare Advantage Plan under Part C and Prescription Drug Plan under Part D has an anti-fraud plan in effect
- States and territories establish Medicaid Recovery Audit Contractors
  - Identify overpayments and underpayments
  - Coordinate efforts with federal and state auditors

5/01/2015
Medicare and Medicaid Fraud and Abuse Prevention
Outreach & Education MEDIC (O&E MEDIC)

- Created the CMS O&E MEDIC website on behalf of the CMS Center for Program Integrity
  - To help those committed to stopping Parts C/D fraud, waste, and abuse, by providing
    - Outreach and education materials
    - Professional education
    - Regulation and guidance
    - Fraud - fighting resources
    - General news

Medicaid Integrity Contractors (MICs)

- Support, not replace, state Medicaid program integrity efforts
- Conduct post-payment audits of Medicaid providers
- Identify overpayments, and refer to the state for collection of the overpayments
- Doesn’t adjudicate appeals, but supports state adjudication process
- Three types of MICs: review, audit, and education
CMS Administrative Actions

- When CMS suspects fraud, administrative actions include the following:
  - Automatic denials of payment
  - Payment suspensions
  - Prepayment edits
  - Civil monetary penalties
  - Revocation of billing privileges
  - Referral to law enforcement
  - Overpayment determinations

Law Enforcement Actions

- When law enforcement finds fraudulent activities, enforcement actions include
  - Providers/companies are barred from the programs
  - Providers/companies can’t bill Medicare, Medicaid, or Children’s Health Insurance Plan (CHIP)
  - Providers/companies are fined
  - Arrests and convictions occur
  - Corporate Integrity Agreements may be negotiated
Health Care Fraud Prevention Partnership

- Includes the federal government, state officials, private health insurance organizations, and other health care anti-fraud groups
  - Shares information and best practices
  - Improves detection
  - Prevents payment of fraudulent health care billings across public and private payers
  - Enables the exchange of data and information among the partners

Health Care Fraud Prevention and Enforcement Action (HEAT) Team

- Joint initiative between U.S. Department of Health & Human Services and U.S. Department of Justice
- Improve interagency collaboration on reducing and preventing fraud in federal health care programs
- Increase coordination, data sharing, and training among investigators, agents, prosecutors, analysts, and policymakers
Medicare Fraud Strike Force Teams

- Medicare Fraud Strike Force Teams
  - Located in fraud “hot spot” locations
  - Use advanced data analysis to identify high-billing levels in health care fraud hot spots
  - Coordinate national takedowns
- CMS supports Strike Force takedowns
  - Perform data analysis
  - Suspends payment

Fraud Prevention Toolkit

- Visit CMS.gov to access the Fraud Prevention Toolkit that includes
  - The 4Rs brochure
  - Fact sheets on preventing and detecting fraud
  - Frequently Asked Questions
- CMS.gov also has information about the Center for Program Integrity and fraud prevention efforts in Medicare fee-for-service, Parts C and D, and Medicaid
Provider and Beneficiary Education

- Provider education helps correct vulnerabilities
  - Maintain proper documentation
  - Reduce inappropriate claims submission
  - Protect patient and provider identity information
  - Establish a broader culture of compliance
- Beneficiary education helps identify and report suspected fraud

Check Your Knowledge—Question 3

When CMS detects fraud, administrative actions may include the following:

a. Civil monetary penalties
b. Revocation of billing privileges
c. Referral to law enforcement
d. All of the above
 Lesson 3—How You Can Fight Fraud

- 4Rs for Fighting Medicare Fraud
- stopmedicarefraud.gov
- Medicare Summary Notices
- MyMedicare.gov
- 1-800-MEDICARE
- Senior Medicare Patrol
- Protecting Personal Information and ID Theft
- Reporting Medicaid Fraud
- Helpful Resources

4Rs for Fighting Medicare Fraud

You’re the first line of defense against Medicare fraud and abuse. Here are some ways you can protect yourself from fraud:

1. Record appointments and services
2. Review services provided
   - Compare services actually received with services on your Medicare Summary Notice
3. Report suspected fraud
4. Remember to protect personal information, such as your Medicare card and bank account numbers
STOPMedicareFraud.gov

- Learn about fraud
- Find resources
- Report fraud online
- Access videos
- See recent Health Care Fraud Prevention and Enforcement Action Team HEAT Task Force results by state

Medicare Summary Notice (MSN)

- CMS redesigned the MSN for Part A and Part B to make it easier to read and spot fraud
- Shows all your services or supplies
  - Billed to Medicare in 3-month period
  - What Medicare paid
  - What you owe
- Read it carefully

05/01/2015 Medicare and Medicaid Fraud and Abuse Prevention 33

5/01/2015 Medicare and Medicaid Fraud and Abuse Prevention 36
MyMedicare.gov

- Secure site to manage personal information
  - Review eligibility, entitlement, and plan information
  - Track preventive services
  - Keep a prescription drug list
- Review claims "if you have Original Medicare"
  - Available almost immediately after they are processed

1-800-MEDICARE (TTY 1-877-486-2048)

- Beneficiary fraud complaints received
  - Help target certain providers/suppliers for review
  - Show where fraud scams are heating up
- Using the Interactive Voice Response System
  - Access up to 15 months of claims
  - Check for proper dates, services, and supplies received
    - If not checking claims on MyMedicare.gov
Learning Activity

John has concerns and wants to discuss his Medicare Summary Notice with you.

What are some things that might indicate fraud?

Learning Activity

What Might Indicate Fraud?

- Was he charged for any medical services he didn’t get?
- Do the dates of services look unfamiliar?
- Was he billed for the same thing twice?
- Does his credit report show any unpaid bills for medical services or equipment you didn’t receive?
- Has he received any collection notices for medical services or equipment he didn’t receive?
Fighting Fraud Can Pay

- You may get a reward if you meet all of these conditions:
  - You call either 1-800-HHS-TIPS (1-800-447-8477) or call 1-800-MEDICARE (1-800-633-4227) to report suspected fraud. TTY users should call 1-877-486-2048.
  - The suspected Medicare fraud you report must be investigated and validated by CMS’s contractors.
  - The reported fraud must be formally referred to the Office of Inspector General for further investigation.
  - You aren’t an excluded individual.
  - The person or organization you’re reporting isn’t already under investigation by law enforcement.
  - Your report leads directly to the recovery of at least $100 of Medicare money.

5/01/2015 Medicare and Medicaid Fraud and Abuse Prevention

The Senior Medicare Patrol

- Education and prevention program aimed at educating beneficiaries on preventing, identifying, and reporting health care fraud
- Active programs in all states, the District of Columbia, Puerto Rico, Guam, and U.S. Virgin Islands
- Seeks volunteers to represent their communities
- Nationwide toll-free number: 1-877-808-2468

5/01/2015 Medicare and Medicaid Fraud and Abuse Prevention
Protecting Personal Information

- Only share with people you trust
  - Doctors, other health care providers, and plans approved by Medicare
  - Insurers who pay benefits on your behalf
  - Trusted people in the community who work with Medicare, like your State Health Insurance Assistance Program (SHIP) or Social Security
- Call 1-800-MEDICARE (1-800-633-4227) if you aren’t sure if a provider is approved by Medicare
  - TTY users should call 1-877-486-2048

Identity Theft

- Identity theft is a serious crime
  - Someone else uses your personal information, like your Social Security or Medicare number
- If you think someone is using your information
  - Call your local police department
  - Call the Federal Trade Commission’s ID Theft Hotline at 1-877-438-4338
- If your Medicare card is lost or stolen, report it right away
  - Call Social Security at 1-800-772-1213
  - TTY users should call 1-800-325-0778
Reporting Suspected Medicaid Fraud

- Medicaid Fraud Control Unit (MFCU) investigates and prosecutes
  - Medicaid fraud
  - Patient abuse and neglect in health care facilities
- Call the Office of the Inspector General at 1-800-447-8477 (TTY 1-800-377-4950)
  - They also certify and annually re-certify the MFCU
- State Medical Assistance (Medicaid) office
  - See state listing for Medicaid
  - Download contacts at oig.hhs.gov/fraud/Medicaid-fraud-control-units-mfcu/files/contact-directors.pdf

Key Points to Remember

- The key difference between fraud and abuse is intention
- Improper payments are often mistakes
- CMS fights fraud and abuse with support from Program Integrity Contractors
- You can fight fraud and abuse with the 4Rs: Record, Review, Report, Remember
- There are many sources of additional information
Medicare Fraud & Abuse Resource Guide

<table>
<thead>
<tr>
<th>Resources</th>
<th>Medicare Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centers for Medicare &amp; Medicaid Services (CMS)</td>
<td>&quot;Medicare Authorization to Disclose Personal Information&quot; form</td>
</tr>
<tr>
<td>1-800-MEDICARE</td>
<td>CMS Product No. 10106</td>
</tr>
<tr>
<td>(1-800-633-4227)</td>
<td>&quot;Help Prevent Fraud: Check Your Medicare Claims Early&quot;</td>
</tr>
<tr>
<td>TTY 1-877-486-2048</td>
<td>CMS Product No. 11491 and No. 11492</td>
</tr>
<tr>
<td>Medicare.gov</td>
<td>&quot;Protecting Medicare and You From Fraud&quot;</td>
</tr>
<tr>
<td>MyMedicare.gov - MyMedicare.gov/</td>
<td>CMS Product No. 10111</td>
</tr>
<tr>
<td>CMS Program Integrity CMS.gov/About-</td>
<td>&quot;Quick Facts About Medicare Plans and Protecting Your Personal Information&quot;</td>
</tr>
<tr>
<td>CMSComponents/EPI/Center-for-program-</td>
<td>CMS Product No. 11147</td>
</tr>
<tr>
<td>integrity.html</td>
<td>&quot;4 Tips for Fighting Fraud&quot;</td>
</tr>
<tr>
<td></td>
<td>CMS Product No. 11610</td>
</tr>
<tr>
<td>STOD/MedicareFraud.gov</td>
<td>&quot;You Can Help Protect Yourself and Medicare From Fraud Committed by Dishonest Suppliers&quot;</td>
</tr>
<tr>
<td>Office of Inspector General hhs.gov/</td>
<td>CMS Product No. 11442</td>
</tr>
<tr>
<td>U.S. Department of Health &amp; Human Services</td>
<td>To access these products:</td>
</tr>
<tr>
<td>ATSC: HOTLINE: hhs.gov/</td>
<td>View and order single copies</td>
</tr>
<tr>
<td>bathemissions/</td>
<td>Medicare.gov/publications</td>
</tr>
<tr>
<td>P.O. Box 23448, Washington, DC 20046</td>
<td>Order multiple copies (partners only):</td>
</tr>
<tr>
<td>Fraud Hotline</td>
<td>productordering.cms.hhs.gov</td>
</tr>
<tr>
<td>1-800-HHS-7869 (1-800-447-8677)</td>
<td>(You must register your organization.)</td>
</tr>
<tr>
<td>TTY 1-800-337-8456</td>
<td></td>
</tr>
<tr>
<td>Fax 1-800-273-8162</td>
<td></td>
</tr>
<tr>
<td>HealthCare.gov</td>
<td></td>
</tr>
<tr>
<td>HealthCare.gov/how-can-i-protect-myself-from-</td>
<td></td>
</tr>
<tr>
<td>fraud-in-the-health-insurance-marketplace/</td>
<td></td>
</tr>
<tr>
<td>Social Security Administration</td>
<td></td>
</tr>
<tr>
<td>SSA.gov</td>
<td></td>
</tr>
<tr>
<td>1-800-772-1213</td>
<td></td>
</tr>
<tr>
<td>TTY 1-800-325-0778</td>
<td></td>
</tr>
<tr>
<td>Senior Medicare Patrol Program</td>
<td></td>
</tr>
<tr>
<td>SMAFPatrol.gov</td>
<td></td>
</tr>
<tr>
<td>find the SMP resources in your state under</td>
<td></td>
</tr>
<tr>
<td>find help: SMP locator</td>
<td></td>
</tr>
<tr>
<td>Fraud Scams</td>
<td></td>
</tr>
<tr>
<td>SMPPatrolResource.org/PSF/integrity/downloads/section</td>
<td></td>
</tr>
<tr>
<td>ppLinkedInTemplate-CMS_VOPHIS/display/doc &amp;ContentID=5512</td>
<td></td>
</tr>
<tr>
<td>NBI Medi's Parts C&amp;F Fraud Reporting Group</td>
<td></td>
</tr>
<tr>
<td>1-877-7SAFER (1-877-772-3379)</td>
<td></td>
</tr>
<tr>
<td>healthintegrity.com/contactus/cbi-</td>
<td></td>
</tr>
<tr>
<td>mediareporting-a-complaint</td>
<td></td>
</tr>
<tr>
<td>Fax a Complaint Form to 410-919-8638</td>
<td></td>
</tr>
<tr>
<td>Mail to: Health Integrity, LLC, 7102</td>
<td></td>
</tr>
<tr>
<td>Ambassador Road, Suite 100, Windsor Mill,</td>
<td></td>
</tr>
<tr>
<td>MD 21044</td>
<td></td>
</tr>
<tr>
<td>Healthintegrity.com/verifacts/cbi-</td>
<td></td>
</tr>
<tr>
<td>medic</td>
<td></td>
</tr>
<tr>
<td>National Health Care Anti-Fraud Assoc.</td>
<td></td>
</tr>
<tr>
<td>NICFA.org</td>
<td></td>
</tr>
<tr>
<td>Medicare beneficiary education</td>
<td></td>
</tr>
<tr>
<td>CMS.gov/Medicare-Medicare-</td>
<td></td>
</tr>
<tr>
<td>Coordination/Fraud-Prevention/Medicare-</td>
<td></td>
</tr>
<tr>
<td>Integrity-Education/content-lending.html</td>
<td></td>
</tr>
<tr>
<td>Prevention Toolkit</td>
<td></td>
</tr>
<tr>
<td>CMS.gov/Outreach-and-Education/Outreach/</td>
<td></td>
</tr>
<tr>
<td>Partnerships/FraudPreventionContent/lending.html</td>
<td></td>
</tr>
<tr>
<td>CMS Outreach &amp; Education MEDIC</td>
<td></td>
</tr>
<tr>
<td>medic-outreach.nationalmakersolutions.com</td>
<td></td>
</tr>
</tbody>
</table>

CMS National Training Program (NTP)

To view all available NTP training materials, or to subscribe to our email list, visit CMS.gov/Outreach-and-Education/Training/CMSNationalTrainingProgram/index.html

For questions about training products, email training@cms.hhs.gov

Fraud and Abuse Prevention 24
Appendix 2a

Code of Ethics and Business Conduct

CMS Fraud and Abuse Guide
Medicare Fraud & Abuse
Prevention, Detection, and Reporting

Medicare Fraud and Abuse: A Serious Problem that Requires Your Attention

Although no precise measure of health care fraud exists, those intent on abusing the system can cost taxpayers billions of dollars while putting beneficiaries' health and welfare at risk. Medicare fraud and abuse increases the strain on the Medicare Trust Fund. The impact of these losses and risks magnify as Medicare continues to serve a growing number of people.

You play a vital role in protecting the integrity of the Medicare Program. To combat fraud and abuse, you need to know what to watch for to protect your organization from potential abusive practices, civil liability, and criminal activity. This fact sheet gives you some of the tools you need to protect the Medicare Program, your patients, and yourself, including:

- Examples of Medicare fraud and abuse;
- Overview of the laws used to fight fraud and abuse;
- Descriptions of the partnerships among government agencies engaged in preventing, detecting, and fighting fraud and abuse; and
- Resources on how you can report suspected fraud and abuse.
You Can Help Fight Fraud – Report It!

For a short video on reporting Medicare fraud to the Office of Inspector General (OIG), visit http://www.youtube.com/watch?v=nH7p3G7dOw or click the image on the left.

What Is Medicare Fraud?

Medicare fraud is typically characterized by:

- Knowingly submitting false statements or making misrepresentations of fact to obtain a federal health care payment for which no entitlement would otherwise exist;
- Knowingly soliciting, paying, and/or accepting remuneration to induce or reward referrals for items or services reimbursed by Federal health care programs; or
- Making prohibited referrals for certain designated health services.

Anyone can commit health care fraud. Fraud schemes range from solo ventures to broad-based operations by an institution or group. Even organized crime has infiltrated the Medicare Program and masqueraded as Medicare providers and suppliers. Examples of Medicare fraud include:

- Knowingly billing for services not furnished, supplies not provided, or both, including falsifying records to show delivery of such items or billing Medicare for appointments that the patient failed to keep; and
- Knowingly billing for services at a level of complexity higher than the service actually provided or documented in the file.

Case Studies

To learn about real-life cases of Medicare fraud and abuse and the consequences for culprits, visit http://www.stopmedicarefraud.gov/newsroom on the Internet.
Defrauding the Federal government and its programs is illegal. Committing Medicare fraud exposes individuals or entities to potential criminal and civil remedies, including imprisonment, fines, and penalties. Criminal and civil penalties for Medicare fraud reflect the serious harms associated with health care fraud and the need for aggressive and appropriate intervention. Providers and health care organizations that commit health care fraud risk exclusion from participation in Federal health care programs and the loss of their professional licenses.

What Is Medicare Abuse?

Abuse describes practices that, either directly or indirectly, result in unnecessary costs to the Medicare Program. Abuse includes any practice that is not consistent with the goals of providing patients with services that are medically necessary, meet professionally recognized standards, and priced fairly.

Examples of Medicare abuse include:

- Billing for services that were not medically necessary;
- Charging excessively for services or supplies; and
- Misusing codes on a claim, such as upcoding or unbundling codes.

Medicare abuse can also expose providers to criminal and civil liability.

Figure 1 shows examples along the spectrum of causes of improper payments.

**Figure 1. Types of Improper Payments**

Program Integrity encompasses a range of activities to target the various causes of improper payments:

- **Mistake**
- **Inefficiencies**
- **Bending the Rules**
- **Intentional Deception**

**Examples:**

- Incorrect coding
- Medically unnecessary service
- Improper Billing practices (such as, upcoding)
- Billing for services or supplies that were not provided
Medicare Fraud and Abuse Laws

Federal laws governing Medicare fraud and abuse include the:

- False Claims Act (FCA);
- Anti-Kickback Statute (AKS);
- Physician Self-Referral Law (Stark Law);
- Social Security Act; and

These bodies of law specify the criminal and/or civil remedies the government can impose upon individuals or entities that commit fraud and abuse in the Medicare Program, including Medicare Parts C and D, as well as the Medicaid Program. Violations of these laws may result in nonpayment of claims, Civil Monetary Penalties (CMPs), exclusion from participation in Federal health care programs, and criminal and civil liability. Liability can exist without proof of actual knowledge or a specific intent to violate the law. We briefly summarize each law below, and you can find hyperlinks to the text of the laws at the end of this section in Table 1.

**False Claims Act (FCA)**
The FCA protects the government from being overcharged or sold substandard goods or services. The FCA imposes civil liability on any person who knowingly submits, or causes the submission of, a false or fraudulent claim to the Federal government. The “knowing” standard includes acting in deliberate ignorance or reckless disregard of the truth related to the claim.

**Example:** A physician submits claims to Medicare for a higher level of medical services than actually provided or that the medical record documents.

**Penalties:** Civil penalties for violating the FCA can include fines of $5,500–$11,000 per false claim and up to three times the amount of damages sustained by the government as a result of the false claims.

There is also a criminal FCA statute by which individuals or entities that submit false claims can face criminal penalties.
Anti-Kickback Statute (AKS)
The AKS makes it a criminal offense to knowingly and willfully offer, pay, solicit, or receive any remuneration directly or indirectly to induce or reward referrals of items or services reimbursable by a Federal health care program.

Example: A provider receives cash or below fair market value rent for medical offices in exchange for referrals.

Penalties: Civil penalties for violating the AKS can include fines up to three times the amount of kickback. Criminal penalties for violating the AKS can include fines, imprisonment, or both.

If certain types of arrangements satisfy regulatory safe harbors, the AKS will not treat these arrangements as offenses. For more information on safe harbors, visit the United States (U.S.) Department of Health & Human Services (HHS) Office of Inspector General’s (OIG) website at https://oig.hhs.gov/compliance/safe-harbor-regulations on the OIG website.
Physician Self-Referral Law (Stark Law)

The Physician Self-Referral Law, often called the Stark Law, prohibits a physician from making a referral for certain designated health services to an entity in which the physician (or member of his or her immediate family) has an ownership/investment interest or with which he or she has a compensation arrangement, unless an exception applies.

**Example:** A provider refers a beneficiary for a designated health service to a business in which the provider has an investment interest.

**Penalties:** Penalties for physicians who violate the Stark Law include fines, repayment of claims, and potential exclusion from participation in all Federal health care programs.

For more information, visit http://www.cms.gov/Medicare/Fraud-and-Abuse/PhysicianSelfReferral on the CMS website.

Criminal Health Care Fraud Statute

The Criminal Health Care Fraud Statute prohibits **knowingly and willfully** executing, or attempting to execute, a scheme or artifice in connection with the delivery of or payment for health care benefits, items, or services to:

- Defraud any health care benefit program; or
- Obtain (by means of false or fraudulent pretenses, representations, or promises) any of the money or property owned by, or under the custody or control of, any health care benefit program.

**Example:** Several doctors and medical clinics conspire in a coordinated scheme to defraud the Medicare Program by submitting claims for power wheelchairs that were not medically necessary.

**Penalties:** Penalties for violating the Criminal Health Care Fraud Statute may include fines, imprisonment, or both.
Additional Medicare Fraud and Abuse Penalties

Aside from the civil and criminal actions brought by law enforcement agencies, the Medicare Program has additional administrative remedies applicable for certain fraud and abuse violations.

Exclusions

Under the Exclusion Statute, the OIG must exclude from participation in all Federal health care programs providers and suppliers convicted of:

- Medicare fraud;
- Patient abuse or neglect;
- Felony convictions related to fraud, theft, embezzlement, breach of fiduciary responsibility, or other financial misconduct in connection with the delivery of a health care item or service; or
- Felony convictions for unlawful manufacture, distribution, prescription, or dispensing of controlled substances.

The OIG also has the discretion to impose exclusions on a number of other grounds. Excluded providers cannot participate in Federal health care programs for a designated period. An excluded provider may not bill Federal health care programs (including, but not limited to, Medicare, Medicaid, and State Children's Health Insurance Program [SCHIP]) for services he or she orders or performs. At the end of an exclusion period, an excluded provider must affirmatively seek reinstatement; reinstatement is not automatic. The OIG maintains a list of excluded parties called the List of Excluded Individuals/Entities (LEIE), at https://oig.hhs.gov/exclusions on the OIG website.

Civil Monetary Penalties Law (CMPL)

Under the CMPL, Civil Monetary Penalties (CMPs) apply for a variety of conduct. The CMPL authorizes penalties of up to $50,000 per violation, and assessments of up to three times the amount claimed for each item or service, or up to three times the amount of remuneration offered, paid, solicited, or received. Violations that may give rise to CMPs include:

- Presenting a claim that you know or should know is for an item or service not provided as claimed or that is false and fraudulent;
- Presenting a claim that you know or should know is for an item or service for which Medicare will not pay; and
- Violating the AKS.
<table>
<thead>
<tr>
<th>Statute</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>31 United States Code (U.S.C.)</td>
<td></td>
</tr>
<tr>
<td>Sections 3729-3733</td>
<td></td>
</tr>
<tr>
<td>18 U.S.C. Section 287</td>
<td></td>
</tr>
<tr>
<td>42 U.S.C. 1320A-7(b)</td>
<td></td>
</tr>
<tr>
<td>42 Code of Federal Regulations (CFR)</td>
<td></td>
</tr>
<tr>
<td>Section 1001.952</td>
<td></td>
</tr>
<tr>
<td>42 U.S.C. Section 1395nn</td>
<td></td>
</tr>
<tr>
<td>18 U.S.C. Section 1347</td>
<td></td>
</tr>
<tr>
<td>42 U.S.C. Section 1320a-7</td>
<td></td>
</tr>
<tr>
<td>42 U.S.C. Section 1320a-7a</td>
<td></td>
</tr>
</tbody>
</table>

**Medicare Fraud and Abuse Partnerships**

Government agencies partner to fight fraud and abuse, uphold the Medicare Program’s integrity, save and recoup taxpayer funds, reduce health care costs, and improve the quality of care.

**Public-Private Health Care Fraud Prevention Partnership**

The Health Care Fraud Prevention Partnership (Partnership) is a public-private forum for the Federal government and private and state organizations, including insurers, to prevent health care fraud on a national scale. Public and private sector partners exchange information and best practices to detect and prevent fraudulent claims and payments. The partnership also performs analytics on industry-wide data to detect and predict fraud schemes. For more information on the partnership, visit [http://www.stopmedicarefraud.gov/aboutfraud/public-private](http://www.stopmedicarefraud.gov/aboutfraud/public-private) on the Internet.
Centers for Medicare & Medicaid Services (CMS)

CMS is the Federal agency responsible for administering the Medicare, Medicaid, State Children’s Health Insurance Program (SCHIP), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Clinical Laboratory Improvement Amendments (CLIA), and several other health-related programs. For more information about CMS and its programs, visit http://www.cms.gov on the CMS website.

To prevent and detect fraud and abuse, CMS partners with individuals, entities, and law enforcement agencies, including:

- Accreditation Organizations (AOs);
- Medicare beneficiaries and caregivers;
- Physicians, suppliers, and other health care providers; and
- State and Federal law enforcement agencies, including the OIG, Federal Bureau of Investigation (FBI), Department of Justice (DOJ), State Medicaid Agencies, and Medicaid Fraud Control Units (MFCUs).

To support its efforts to prevent, detect, and investigate potential Medicare fraud and abuse, CMS also contracts with an array of contractors, including:

- Comprehensive Error Rate Testing (CERT) Contractors;
- Medicare Administrative Contractors (MACs) which pay claims and enroll providers and suppliers;
- Medicare Drug Integrity Contractors (MEDICs);
- Recovery Audit Program Recovery Auditors; and
- Zone Program Integrity Contractors (ZPICs), formerly called Program Safeguard Contractors (PSCs), which investigate potential fraud and abuse.

The Center for Program Integrity (CPI), within CMS, promotes the integrity of Medicare through audits, policy reviews, and identification and monitoring of program vulnerabilities. CPI oversees CMS’ collaborative interactions with key stakeholders on program integrity issues related to the detecting, deterring, monitoring, and combating fraud and abuse. For the latest CPI news, visit http://blog.cms.gov/category/cms-center-for-program-integrity on the CMS website.
In 2010, HHS and CMS launched an ambitious national effort to obstruct criminals at every step in the act of committing fraud. The Fraud Prevention System (FPS) is the state-of-the-art predictive analytics technology that runs predictive algorithms and other analytics nationwide on all Medicare Fee-For-Service (FFS) claims prior to payment. For the first time in Medicare history, CMS systematically applies advanced analytics to the Medicare FFS claims on a streaming, nationwide basis.

In 2012, CMS created the Program Integrity Command Center to bring together officials, experts, and investigators from Medicare, Medicaid, and the law enforcement community, including the OIG and FBI. The Command Center gathers experts in one room to develop intricate predictive analytics identifying fraud and mobilizing a rapid fraud response. CMS uses this technology to connect instantly with its field offices and evaluate fraud allegations through real-time investigations. Previously, finding substantiating evidence of a fraud allegation took days or weeks; now it takes mere hours.

Office of Inspector General (OIG)
The OIG protects the integrity of HHS’ programs, including Medicare, and the health and welfare of its beneficiaries. The OIG carries out its duties through a nationwide network of audits, investigations, inspections, and other related functions. The Inspector General has the authority to exclude individuals and entities who engage in fraud or abuse from participation in Medicare, Medicaid, and other Federal health care programs and to impose CMPs for certain misconduct related to Federal health care programs.

Health Care Fraud Prevention and Enforcement Action Team (HEAT)
The DOJ and HHS established HEAT to build and strengthen existing programs combatting Medicare fraud while investing new resources and technology to prevent fraud and abuse. HEAT efforts included expansion of the DOJ-HHS Medicare Fraud Strike Force, which successfully fights fraud. HEAT created the Stop Medicare Fraud website, which provides information about how to identify and protect against Medicare fraud and how to report it. For more information on HEAT, visit http://www.stopmedicarefraud.gov on the Internet.

General Services Administration (GSA)
The GSA consolidated several Federal procurement systems into one new system—the System for Award Management (SAM). SAM incorporated the formerly maintained Excluded Parties List System (EPLS). SAM includes information on entities debarred, suspended, proposed for debarment, excluded, or disqualified from receiving Federal contracts or certain subcontracts and from certain types of Federal financial and non-financial assistance and benefits. For more information on excluded parties, visit https://www.sam.gov on the Internet.
Report Suspected Fraud

The following table tells you how to report Medicare fraud.

Table 2. Where Should You Report Fraud and Abuse?

<table>
<thead>
<tr>
<th>If You Are a...</th>
<th>Report Fraud to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medicare Beneficiary</td>
<td>For any complaint:</td>
</tr>
<tr>
<td></td>
<td>- CMS Hotline:</td>
</tr>
<tr>
<td></td>
<td>Phone: 1-800-MEDICARE (1-800-633-4227) or</td>
</tr>
<tr>
<td></td>
<td>TTY 1-877-486-2048; or</td>
</tr>
<tr>
<td></td>
<td>- OIG Hotline:</td>
</tr>
<tr>
<td></td>
<td>Phone: 1-800-HHS-TIPS (1-800-447-8477) or</td>
</tr>
<tr>
<td></td>
<td>TTY 1-800-377-4950;</td>
</tr>
<tr>
<td></td>
<td>Fax: 1-800-223-8164;</td>
</tr>
<tr>
<td></td>
<td>Email: <a href="mailto:HHSTips@oig.hhs.gov">HHSTips@oig.hhs.gov</a></td>
</tr>
<tr>
<td></td>
<td>Online: <a href="https://forms.oig.hhs.gov/hotlineoperations">https://forms.oig.hhs.gov/hotlineoperations</a></td>
</tr>
<tr>
<td></td>
<td>Mail: U.S. Department of Health &amp; Human Services</td>
</tr>
<tr>
<td></td>
<td>Office of Inspector General</td>
</tr>
<tr>
<td></td>
<td>Attn: OIG Hotline Operations</td>
</tr>
<tr>
<td></td>
<td>P.O. Box 23489</td>
</tr>
<tr>
<td></td>
<td>Washington, DC 20026</td>
</tr>
<tr>
<td></td>
<td>OR</td>
</tr>
<tr>
<td></td>
<td>For Medicare Part C (Managed Care) or Part D (Prescription Drug Plans) complaints:</td>
</tr>
<tr>
<td></td>
<td>- 1-877-7SafeRx (1-877-772-3379)</td>
</tr>
</tbody>
</table>
Table 2. Where Should You Report Fraud and Abuse? (cont.)

<table>
<thead>
<tr>
<th>If You Are a...</th>
<th>Report Fraud to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medicare Provider</td>
<td>• OIG Hotline:</td>
</tr>
<tr>
<td></td>
<td>Phone: 1-800-HHS-TIPS (1-800-447-8477) or TTY 1-800-377-4950;</td>
</tr>
<tr>
<td></td>
<td>Fax: 1-800-223-8164;</td>
</tr>
<tr>
<td></td>
<td>Email: <a href="mailto:HHSTips@oig.hhs.gov">HHSTips@oig.hhs.gov</a></td>
</tr>
<tr>
<td></td>
<td>Online: <a href="https://forms.oig.hhs.gov/hotlineoperations">https://forms.oig.hhs.gov/hotlineoperations</a></td>
</tr>
<tr>
<td></td>
<td>Mail: U.S. Department of Health &amp; Human Services</td>
</tr>
<tr>
<td></td>
<td>Office of Inspector General</td>
</tr>
<tr>
<td></td>
<td>Attn: OIG Hotline Operations</td>
</tr>
<tr>
<td></td>
<td>P.O. Box 23489</td>
</tr>
<tr>
<td></td>
<td>Washington, DC 20026</td>
</tr>
<tr>
<td>OR</td>
<td>• Your local MAC</td>
</tr>
<tr>
<td></td>
<td>For MAC contact information, visit <a href="http://www.cms.gov/">http://www.cms.gov/</a></td>
</tr>
<tr>
<td></td>
<td>Research-Statistics-Data-and-Systems/Monitoring-Programs/</td>
</tr>
<tr>
<td></td>
<td>Medicare-FFS-Compliance-Programs/Review-Contractor-Directory-Interactive-Map on</td>
</tr>
<tr>
<td>Medicaid Beneficiary or Provider</td>
<td>the CMS website.</td>
</tr>
<tr>
<td></td>
<td>• OIG Hotline</td>
</tr>
<tr>
<td></td>
<td>Phone: 1-800-HHS-TIPS (1-800-447-8477) or TTY 1-800-377-4950</td>
</tr>
<tr>
<td></td>
<td>Fax: 1-800-223-8164</td>
</tr>
<tr>
<td></td>
<td>Email: <a href="mailto:HHSTips@oig.hhs.gov">HHSTips@oig.hhs.gov</a></td>
</tr>
<tr>
<td></td>
<td>Online: <a href="https://forms.oig.hhs.gov/hotlineoperations">https://forms.oig.hhs.gov/hotlineoperations</a></td>
</tr>
<tr>
<td></td>
<td>Mail: U.S. Department of Health &amp; Human Services</td>
</tr>
<tr>
<td></td>
<td>Office of Inspector General</td>
</tr>
<tr>
<td></td>
<td>Attn: OIG Hotline Operations</td>
</tr>
<tr>
<td></td>
<td>P.O. Box 23489</td>
</tr>
<tr>
<td></td>
<td>Washington, DC 20026</td>
</tr>
<tr>
<td>OR</td>
<td>• Your Medicaid State Agency</td>
</tr>
<tr>
<td></td>
<td>State MFCUs are listed at <a href="http://www.cms.gov/">http://www.cms.gov/</a></td>
</tr>
<tr>
<td></td>
<td>Medicare-Medicaid-Coordination/Fraud-Prevention/</td>
</tr>
<tr>
<td></td>
<td>FraudAbuseforConsumers/Report_Fraud_and_Suspected_Fraud.html on the CMS website.</td>
</tr>
</tbody>
</table>
If you prefer, you can give your complaint anonymously to the OIG Hotline; the OIG record systems will contain no information that could trace the complaint to you. This lack of contact information, however, may prevent OIG’s comprehensive review of the complaint. So, the OIG encourages you to provide contact information for possible follow-up.

Medicare and Medicaid beneficiaries can learn more about protecting themselves and spotting fraud by contacting their local Senior Medicare Patrol (SMP) program. For more information about SMP or to find the local SMP, visit the SMP Locator at http://www.smpresource.org on the Internet.

For questions about Medicare billing procedures, billing errors, or questionable billing practices, contact your MAC. For MAC contact information, including toll-free telephone numbers, visit http://www.cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/Medicare-FFS-Compliance-Programs/Review-Contractor-Directory-Interactive-Map on the CMS website.
Resources

For more information about the OIG and fraud, visit [https://oig.hhs.gov/fraud](https://oig.hhs.gov/fraud) on the OIG website, or scan the Quick Response (QR) code on the right with your mobile device. For more information regarding preventing, detecting, and reporting Medicare fraud and abuse, refer to the resources listed below.

Table 3. Fraud and Abuse Resources

<table>
<thead>
<tr>
<th>Resource</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>HHS</td>
<td><a href="http://www.hhs.gov">http://www.hhs.gov</a></td>
</tr>
<tr>
<td>OIG</td>
<td><a href="http://oig.hhs.gov">http://oig.hhs.gov</a></td>
</tr>
<tr>
<td>Resource</td>
<td>Website</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CMS Fraud Prevention Toolkit</td>
<td><a href="http://www.cms.gov/Outreach-and-Education/Outreach/Partnerships/">http://www.cms.gov/Outreach-and-Education/Outreach/Partnerships/</a></td>
</tr>
<tr>
<td></td>
<td>FraudPreventionToolkit.html</td>
</tr>
<tr>
<td></td>
<td>NOTE: To access this program, you need to create a free account.</td>
</tr>
<tr>
<td>Products</td>
<td>MLNProductos/Downloads/SafeMed-ID-Products.pdf</td>
</tr>
<tr>
<td></td>
<td>MLNProductos/ProviderCompliance.html</td>
</tr>
<tr>
<td>OIG Advisory Opinions</td>
<td><a href="https://oig.hhs.gov/compliance/advisory-opinions">https://oig.hhs.gov/compliance/advisory-opinions</a></td>
</tr>
<tr>
<td>OIG Compliance 101</td>
<td><a href="https://oig.hhs.gov/compliance/101">https://oig.hhs.gov/compliance/101</a></td>
</tr>
<tr>
<td>OIG Email Updates</td>
<td><a href="https://oig.hhs.gov/contact-us">https://oig.hhs.gov/contact-us</a></td>
</tr>
<tr>
<td></td>
<td>NOTE: To access this program, you need to create a free account.</td>
</tr>
</tbody>
</table>
This fact sheet was current at the time it was published or uploaded onto the web. Medicare policy changes frequently so links to the source documents have been provided within the document for your reference.

This fact sheet was prepared as a service to the public and is not intended to grant rights or impose obligations. This fact sheet may contain references or links to statutes, regulations, or other policy materials. The information provided is only intended to be a general summary. It is not intended to take the place of either the written law or regulations. We encourage readers to review the specific statutes, regulations, and other interpretive materials for a full and accurate statement of their contents.

The Medicare Learning Network® (MLN), a registered trademark of CMS, is the brand name for official information health care professionals can trust. For additional information, visit the MLN’s web page at http://go.cms.gov/MLNGenInfo on the CMS website.

Your feedback is important to us and we use your suggestions to help us improve our educational products, services and activities and to develop products, services and activities that better meet your educational needs. To evaluate Medicare Learning Network® (MLN) products, services and activities you have participated in, received, or downloaded, please go to http://go.cms.gov/MLNProducts and in the left-hand menu click on the link called ‘MLN Opinion Page’ and follow the instructions. Please send your suggestions related to MLN product topics or formats to MLN@cms.hhs.gov.