

BUSINESS ETHICS AND COMPLIANCE PROGRAM

Revised June 1, 2011

(Confidential and proprietary/not to be disclosed to third parties)



TABLE OF CONTENTS

TABLE OF CONTENTS	i & ii
REFERENCE INFORMATION	iii
Compliance Officer	
Compliance Hotline	
MISSION OF THE COMPLIANCE PROGRAM	Tab 1
Business Ethics Policy	
STRUCTURE OF THE COMPLIANCE PROGRAM	Tab 2
Scope and Jurisdiction of the Compliance Program	
Definition of Personnel	
Compliance Program Leadership	
Elements of the Center Compliance Program	
GENERAL COMPLIANCE POLICIES	Tab 3
Participation in Compliance Program Activities	3.1
Duty to Report	3.2
Policy Against Retaliation	3.3
Manager’s Responsibilities Related to the Compliance Program	3.4
Conflicts of Interest	3.5
Use of Corporate Assets	3.6
Limitation on Hiring or Contracting; Background Investigations	3.7
New Partnerships & Acquisitions- Due Diligence	3.8
Anti-trust Compliance.	3.9
Business Gifts & Courtesies	3.10
Travel, Meals & Entertainment.	3.11
Government & Political Interactions	3.12
Financial Reporting Integrity	3.13
Integrity of Data Systems.	3.14
Record Retention.	3.15
Responding to Government Investigation	3.16
Intellectual Property & Confidential Information	3.17

E-Mail Security	3.18
Internet Security.	3.19
Remote Worker Access	3.20

GENERAL BILLING POLICIES Tab 4

Prohibition on Making False Statements on Any Government Or Private Document	4.1
Ambiguity in Physician Documentation for Billing	4.2
Documentation of Medical Necessity.	4.3
Upcoding and Unbundling.	4.4
Responsibility for Coding Updates.	4.5
Medicare as Secondary Payer.	4.6
Inappropriate Balance Billing	4.7
Advance Beneficiary Notice.	4.8
Reviewing Denials, Rejections and Write-offs.	4.9
Waiver of Patient Co-payments, Coinsurance & Deductibles	4.10
Uncompensated Care	4.11
Transfer to External Collection Agency	4.12
Medical Records Release	4.13
Fee Schedules	4.14
Refunds and Overpayments	4.15

OVERVIEW OF RELEVANT LAWS Tab 5

Medicare/Medicaid Anti-Kickback Law	
Stark Law (Physician Self –Referral Prohibition)	
State Self-Referral Bans	
State Fee Splitting Prohibitions	
Federal False Claims Act	
False Statements under the Social Security Act-Criminal	
False Statements under the Social Security Act-Civil	
General Healthcare Fraud Offense	
Mail and Wire Fraud	
False Claims to Insurance Companies	
State False Claims Acts	

REFERENCE INFORMATION

{Each Center will complete }

COMPLIANCE OFFICER:

Karen Sablyak
Physicians Endoscopy, LLC
1456 Ferry Road, Suite 305
Doylestown, PA 18901

Telephone: 215.589.9001
Fax: 215.589.9030

Email: ksablyak@endocenters.com

COMPLIANCE HOTLINE PHONE NUMBER (SEE ALSO POLICY 3.2):

1-877-874-8415 *(Operated by National Hotline Services, Inc.)*

TAB 1
MISSION OF THE COMPLIANCE PROGRAM

Physicians Endoscopy (“PE” or “Company”) is committed to maintaining an environment that promotes ethical conduct. As an expression of this organizational commitment, PE has adopted the following Business Ethics Policy.

Business Ethics Policy

PE is committed to maintaining a work environment and relationships with our physicians, staff and owners that will promote the highest ethical standards of business. Good business practices demand respect for and compliance with the law. PE believes that compliance with the law is a serious matter, and a matter that is the responsibility, without exception, of all Personnel, which is defined in Tab 2 to include, but is not limited to PE employees, owners, Officers, Board of Managers, independent contractors (as applicable, e.g. temporary help), and Committee members. PE is committed to educating its Personnel on the law and on how to comply with both the law and with corporate policies. Because complying with the law is of critical importance to the mission of PE, and because complying with corporate policies is vital to the effectiveness of operations of PE, it is the policy of this organization that Personnel will be subject to disciplinary action for failure to comply with either the law or our corporate policies. Furthermore, all Personnel are encouraged to report any misconduct to the PE Compliance Officer without fear of retaliation.

To promote compliance with the obligations created by the Business Ethics Policy, PE has created and implemented a Compliance Program. The Compliance Program is designed to prevent, detect and remedy both intentional and inadvertent violations of law or corporate policy. In many cases, the compliance program policies are even more restrictive than law in order to eliminate subjectivity regarding compliance obligations and to minimize even the appearance of impropriety.

Exhibits:

Certification of Receipt of Compliance Program

Code of Business Ethics and Compliance Program Annual Compliance Certification

I understand that a copy of the Code of Business Ethics and Compliance Program is available at www.endocenters.com/pe-online for my reference.

I certify that I have attended Compliance Training regarding PE's Code of Business Ethics and Legal Compliance and that I have read and will comply with the Compliance Program standards, policies and procedures;

I further certify that, except as specified below, I have complied with all of the provisions of the Compliance Program during the past year and have no knowledge or reason to believe that any PE employee has violated any provisions of the Program during the past year (statement applicable to existing employees and not new employees);

I understand that any individual who fails to report the violation of any provision of the Compliance Program may face disciplinary action, up to and including termination of employment.

EXCEPTION: _____

(Please attach additional sheet(s) if necessary.)

Signature

Today's Date

Employee's Name/Position

TAB 2
STRUCTURE OF THE COMPLIANCE PROGRAM

Scope and Jurisdiction of the Compliance Program

The PE Compliance Program is designed to promote an understanding of and compliance with the laws and regulations that govern PE operations and its relationships with affiliated Centers, the physicians who use them, owners, employees and other third parties, including, but not limited to:

- State and Federal Dept of Health or other healthcare licensing Agencies which dictate physical plant requirements as well as operating standards
- Medicare/Medicaid which imposes standards and reporting requirements as conditions of participation
- Certificate of Need Requirements (where applicable) which regulate the establishment, expansion and change of ownership of healthcare entities
- Accreditation organization standards (e.g. AAAHC) which PE voluntarily has chosen to achieve

All reporting and investigation procedures contained herein also apply to various other policy and procedure manuals, including but not limited to:

HIPAA Manual

Billing Policies & Procedures

Financial Policies & Procedures

The above manuals are incorporated herein by reference.

Definition of PE Personnel

Obligations imposed by the Compliance Program extend to all PE Personnel. Throughout this Compliance Manual, “PE Personnel” or “Personnel” is defined as all PE employees, independent contractors (e.g. temporary help), officers, owners, Managers of the Board (aka BOM) and Committee members as they carry out their responsibilities on behalf of PE.

Compliance Program Leadership

The Compliance Program was created at the direction of the PE management team and our Board of Managers. The PE President appoints a Compliance Officer, whose appointment is confirmed by the Owners of PE. The Compliance Officer reports directly to the President and to

the Board of Managers on Compliance Program matters. The Compliance Officer oversees implementation and operation of the Compliance Program, and has primary responsibility for investigating allegations of non-compliance with Compliance Program policies. When circumstances warrant, the Compliance Officer may delegate responsibility to or solicit assistance from appropriate PE staff or other individuals to conduct investigations, monitor compliance or implement remediation. A Compliance Committee appointed by the President and approved by the Board of Managers provides direction and assistance to the Compliance Officer.

The Compliance Committee reviews all reports of suspected non-compliance. The Compliance Committee also reviews the findings of compliance investigations and consults with the Compliance Officer regarding corrective action plans to address non-compliance with Compliance Program policies. The Compliance Committee will meet no less than two times per year.

The Compliance Officer is available to help anyone to understand and follow standards set out in this Compliance Manual. Individuals who have questions about the Compliance Program may contact the Compliance Officer (contact information can be found on page “iii”).

Elements Of The Compliance Program

Important elements of the Compliance Program include:

- ***Written policies designed to explain, and prevent violation of, legal requirements.*** The Compliance Program incorporates policies to promote compliance with the most important legal requirements applicable to PE’s business. Many of these policies impose even higher standards than are required under law in order to avoid even the appearance of impropriety. All Personnel must review and understand the Compliance Manual, including the *General Compliance Policies* found behind Tab 3, *Compliance Policies related to Billing* found behind Tab 4, as well as the *Overview of Relevant Laws* found behind Tab 5.
- ***A training program designed to educate PE Personnel on laws, rules and PE policies relevant to their job function.*** All Personnel are required to participate in basic, annual training on the Compliance Program. New hires undergo compliance training as part of their orientation process. PE Personnel whose job functions require understanding of specific compliance policies, such as persons involved in the collection of patient demographic and insurance information as well as clinical information such as CPT and ICD-9 coding used for billing purposes, will also receive training and education to ensure that they understand and comply with those specific compliance policies. In particular, billing and coding personnel will receive regular training related to coding and billing each year. Compliance training may take various forms including live or video taped training sessions. The Compliance Officer will keep track of who has completed training requirements, and employees attending compliance training should always be certain to sign in. Participation in

required compliance training is a condition of continued employment or credentialing at PE.

- ***Monitoring activities designed to ensure that legal requirements and PE policies are properly understood and followed.*** The Compliance Officer and/or his/her designee will monitor organizational activities to ensure that compliance policies are being followed by PE Personnel. Monitoring activities are conducted both as a matter of course (according to an annual monitoring plan), and as follow-up if non-compliant activity is discovered and corrected. Follow-up reviews are designed to ensure that changes made in PE operations to promote compliance have the desired effect of eliminating non-compliant activity.
- ***Monitoring changes in laws, regulations and rules, and communicating relevant changes to Personnel.*** The laws and rules that affect PE's operations can change frequently. Changes in laws or rules may necessitate changes in compliance policies. Creation of new compliance policies also may be required. The Compliance Officer (with assistance from legal counsel and managers in their areas of responsibility) monitors changes in laws and rules that may affect the Compliance Program, and communicates relevant changes to affected personnel.
- ***Investigation of alleged illegal or unethical conduct and recommendations for corrective action when actual illegal or unethical conduct is found.*** All Personnel are obligated to notify a supervisor or the Compliance Officer of known or suspected illegal conduct, or activities that violate PE's compliance policies. When the Compliance Officer receives an allegation of illegal conduct related to an area that is covered by the Compliance Program, he/she will investigate or appoint appropriate personnel to investigate the allegation to determine whether the conduct reported or suspected has actually occurred. The Compliance Officer will report the results of all investigations to the Compliance Committee, which may direct additional follow-up. When non-compliant conduct is found, the Compliance Officer will recommend and assist in implementing corrective action in accordance with this policy. Where necessary, policies will be strengthened, and new policies created, to prevent similar misconduct from occurring in the future.
- ***Discipline or sanctions of Personnel who fail to comply with legal requirements and PE compliance policies.*** Personnel who violate PE's Compliance policies or legal requirements will be subject to disciplinary action. Discipline will be dispensed consistently based upon the nature, severity and frequency of the violation, and not upon the seniority or rank of the violator. Discipline or sanctions may include any of the following:

- Verbal Warning
- Written Warning
- Probationary Monitoring
- Suspension
- Discharge
- Contract Termination
- Restitution

Corporate officers, managers and other persons with managerial or supervisory authority (together, “Managers”) may be held accountable for failing to comply with or for the foreseeable failure of their subordinates to adhere to the applicable standards, laws, rules, program instructions and procedures.

In most situations, discipline of PE Personnel should be progressive, beginning with a verbal warning and proceeding to written warning, suspension, and finally discharge. However, in severe cases, warnings may be bypassed and immediate suspension or discharge may be appropriate.

PE Managers and the Compliance Officer have the authority to issue verbal warnings (provided that the manager notifies the Compliance Officer that a warning has been issued). In addition, the Compliance Officer, following consultation with the Compliance Committee will be responsible for issuing written reprimands, suspensions, discharges, terminations and restitution following approval by PE management.

Tab 3 GENERAL COMPLIANCE POLICIES		
3.1 Participation in Compliance Program Activities		
Effective Date: 12/1/04	Last Revision Date: 2/1/07	By: PE

Policy:

All Personnel, as defined in Tab 2 under Scope and Jurisdiction of the Compliance Program, are required to participate in compliance program activities.

Procedures:

The level and amount of participation required will vary depending on each individual’s activities and responsibilities at PE. At a minimum, participation includes:

1. Reviewing the Compliance Manual (as updated from time to time) and returning a signed statement to the PE Compliance Officer certifying that the individual has received, read and understands the Compliance Manual, at least annually;
2. Reviewing all additions and revisions of Compliance Policies upon receipt;
3. Completing all compliance training assigned to the individual. Assigned training will include at least annual general compliance training for all PE employees and may include more specific compliance training for individuals whose activities and job duties may result in greater risk of non-compliant activity;
4. Complying with Compliance Policies and applicable law when acting on behalf of PE; and
5. Reporting any activity involving Personnel or independent contractors that the individual either knows or in good faith believes is in violation of any legal requirement or PE policy. **[See Policy 3.2 regarding Duty to Report Non-Compliance]**

Failure or refusal to participate in any compliance program activity or to comply with any compliance policy or applicable law may result in discipline, which may include termination of the individual’s employment or contractual relationship with PE.

Tab 3 GENERAL COMPLIANCE POLICIES		
3.2 Duty to Report		
Effective Date: 12/1/04	Last Revision Date: 2/1/07	By: PE

Policy:

Personnel are obligated to report any activity by a PE officer, board member, employee, physician, contractor or other Center staff that appears to violate the law or PE’s compliance policy.

Procedures:

Reports of such non-compliant activity may be made to:

1. A PE Manager;
2. The PE Compliance Officer (contact information can be found on page “iii” in front of the manual behind the Table of Contents)
3. The Compliance Hotline (telephone number can be found on page “iii” in front of the manual behind the Table of Contents)

Individuals who desire to make an anonymous report to the Compliance Officer may use the Report of Suspected Non-Compliance form attached as an exhibit to this policy. If a Manager fails to promptly address a report of potential non-compliant activity, the individual reporting the activity is obligated to report it to the Compliance Officer.

Exhibits:

Report of Suspected Non-Compliance

REPORT OF SUSPECTED NON-COMPLIANCE

The success of PE’s Compliance Program depends largely on free and open reporting of suspected non-compliance by personnel at every level of the organization. Accordingly, we appreciate your report of suspected non-compliance. The Company strictly prohibits retaliation against those who report a potential violation in good faith, even when an investigation determines that no violation occurred. (However, persons who knowingly fabricate compliance reports may be subject to discipline.)

If you suspect non-compliance, please complete this form and submit it to the Compliance Officer (contact information may be found on page “iii” in the front of the manual behind the Table of Contents). Subject to compliance program procedures and applicable law, this form will remain confidential. Although you may file this report on an anonymous basis, your contact information will allow the Compliance Officer to contact you with any follow up questions.

Date of Report:	Date of Incident:	Location/Department Involved:
Name of potential violator:		
Brief description of issue (please attach additional pages or documentation, as deemed necessary and be as specific as possible):		
OPTIONAL: May we contact you if we have follow-up questions? If so, please provide your name and telephone number below: Name: _____ Phone: _____		

Tab 3 GENERAL COMPLIANCE POLICIES		
3.3 Policy Against Retaliation		
Effective Date:12/1/04	Last Revision Date: 2/1/07	By: PE

Policy:

PE strictly prohibits retaliation against persons for reports made in good faith about potential non-compliant activities at PE or any affiliated entity.

Procedures:

Retaliation against any person who reports a compliance concern in good faith is strictly prohibited even if, after investigating the reported concern, it is determined that no real problem exists. For purposes of this policy, retaliation includes any of the following actions:

- Reducing or restricting a person’s duties and/or responsibilities;
- Failing to promote or to give a raise to a person who, were it not for the report of non-compliant activity, would have received a promotion or raise;
- Terminating a person’s employment or office; or
- Taking any other action that is intended to retaliate against or “pay back” a person for a report of non-compliance.

The prohibition against retaliation applies whether the potential non-compliant activity is reported to the compliance hotline, a Manager, the PE Compliance Officer, a member of the Compliance Committee or to the government.

Tab 3 GENERAL COMPLIANCE POLICIES		
3.4 Manager's Responsibilities Related to Compliance Program		
Effective Date: 12/1/04	Last Revision Date: 2/1/07	By: PE

Policy:

PE Managers/Supervisors are responsible for implementing, promoting and supporting PE's Compliance Program in their area of responsibility. Each is responsible for notifying the Compliance Officer of any potential legal or compliance policy violations reported by a subordinate. Every Manager's job performance evaluation will include an evaluation of the Manager's adherence to the requirements of this policy.

Procedures:

The following factors will be evaluated in determining the level of each Manager's effectiveness in implementing, promoting, and adhering to PE's Compliance Program:

1. **Participation in Compliance Program Activities.** The Manager's participation in the Compliance Program activities required of all PE personnel, as required by the policy entitled *Participation in Compliance Program Activities*.
2. **Promotion of Compliance Program.** Manager's performance evaluations will consider overall effort and tone in promoting and supporting compliance activities in their area of responsibility. The Manager's knowledge and understanding of the Compliance Program and of potential compliance issues that may arise in their area of responsibility are essential pre-requisites to effective promotion.
3. **Education and Training of Staff.** Managers will help ensure that individuals who report to them or work in their area of responsibility complete assigned compliance training.
4. **Implementation of Needed Compliance Policies.** In some cases, departments within the Center may be required to institute their own compliance policies that are consistent with PE policy and address issues specific to the department. Managers will participate in the creation of needed departmental compliance policies upon request.
5. **Timely Correction of Discovered Violations.** If a violation of applicable policies or legal requirements is discovered in the Manager's area of responsibility, the Manager must participate in and facilitate correcting the violation in a timely manner, and must take all reasonable steps required to ensure that similar future violations do not occur.

Tab 3 GENERAL COMPLIANCE POLICIES		
3.5 Conflicts of Interest		
Effective Date: 12/1/04	Last Revision Date: 2/1/07	By: PE

Policy:

Personnel will not place themselves in situations where their personal or business interests or the interests of their family could be in conflict with or adversely affect the best interests of PE without the PE’s authorization. Each such person has the duty to disclose conflicts or potential conflicts and to refrain from actions that conflict with PE’s interests. While it is impossible to identify all potential conflicts of interest, the following are examples of situations that can result in a conflict of interest:

- Having a substantial Financial Interest in a supplier or competitor of PE or a Center;
- Having an interest in a transaction in which PE is, or may be, interested;
- Taking advantage of PE’s business opportunities for personal profit; or
- Receiving fees, commissions, or other compensation from a supplier or competitor of PE.

This policy establishes procedures to ensure that Personnel avoid conflicts of interest that adversely affect the Company or its reputation.

I. Definitions

- A. **Interested Person.** Personnel who have a direct or indirect Financial Interest, as defined below, is an Interested Person.
- B. **Financial Interest: Legal Conflict of Interest.** A person has a Financial Interest that constitutes a legal conflict of interest if the person (or an immediate family member) has, directly or indirectly –
1. an ownership or investment interest in any entity [other than the Centers] with which the Company has a transaction or arrangement, or
 2. a compensation arrangement with any entity or individual with which PE has a transaction or arrangement, or
 3. a potential ownership or investment interest in, or compensation arrangement with, any entity [other than the Centers] or individual with which PE is negotiating a transaction or arrangement, or
 4. is an officer, director, manager, general partner, member, employee, independent contractor, consultant, or member of a policy-making committee of the other entity [other than the Centers] in the transaction.

Compensation includes direct and indirect remuneration as well as gifts or favors that are substantial in nature. A conflict of interest will not be deemed to arise from an ownership or other beneficial interest of five percent (5%) or less in a publicly traded company or as a result of investments made through a 401(k) money manager.

- C. **Financial Interest: Business Conflict of Interest.** A person has a Financial Interest which constitutes a business conflict of interest if the person (or an immediate family member) has, directly or indirectly –
1. an ownership or investment interest in any entity which competes with PE or any of its affiliates (including the Centers), or
 2. a compensation arrangement with any entity or individual that competes with PE or any of its affiliates (including the Centers), or
 3. is an officer, director, manager, employee, general partner, member, employee, independent contractor, consultant, or member of a policy-making committee of any entity that competes with PE or any of its affiliates (including the Centers) .

A business conflict will not be deemed to arise from an ownership or other beneficial interest of five percent (5%) or less in a publicly traded company or as a result of investments made through a 401(k) money manager.

II. Procedures for All Personnel:

- A. **General Policy.** While PE respects the right of its Personnel to manage their investments and participate in outside activities, all Personnel should avoid situations that present or create the appearance of a potential conflict between their individual interests (or those of immediate family members) and those of the Company, absent approval by PE.
- B. **Annual Disclosure Statement and Certification.**
1. **Annual Disclosure Statement.** All Personnel shall be required to annually complete and file with the Company, within twenty-eight (28) calendar days of a request from the Company to do so, a disclosure statement identifying interests or relationships as requested in the disclosure statement.
 2. **Annual Certification.** All Personnel shall annually sign a statement that affirms that such person
 - a. has received a copy of the conflicts of interest policy,
 - b. has read and understands the policy, and

- c. has agreed to comply with the policy.
- 3. **Review of Annual Disclosure Statements and Report to the Board.** The annual disclosure statements will be reviewed by the Compliance Officer to determine whether any of the disclosures warrant follow-up actions, such as the divestiture of an ownership interest or termination of a contractual relationship with a supplier or competitor. In addition, the annual disclosure statements of officers, owners, Managers of the PE Board, and senior executive team will be circulated in a packet to the PE Board of Managers.
- 4. **Prior Approval of Additional Financial Interests.** Prior to acquiring any additional Financial Interests that might constitute a Legal Conflict of Interest or Business Conflict of Interest, all Personnel will notify the Compliance Officer of the potential Financial Interest. The Interested Person will not acquire the Financial Interest without the Compliance Officer's approval. When in doubt, individuals should err on the side of reporting the potential conflict and obtaining PE's permission prior to pursuing the transaction or arrangement in question.

III. Additional Procedures for Board Members, Committee Members and Officers

- A. **Duty to Disclose.** In connection with any action, transaction or arrangement by or on behalf of PE that might give rise to an actual or possible conflicts of interest, an Interested Person must disclose the existence of his/her Financial Interest and all material facts to the board and members of committees with board delegated powers considering the proposed transaction, arrangement or board or committee action.
- B. **Determining Whether a Conflict of Interest Exists.** After disclosure of the Financial Interest and all material facts, and after any discussion with the Interested Person, he/she shall leave the board or committee meeting while the determination of a conflict of interest is discussed and voted upon. The remaining board or committee members shall decide if a conflict of interest exists.
- C. **Procedures for Addressing the Conflict of Interest.**
 - 1. An Interested Person may make a presentation at the board or committee meeting, which presentation shall be limited to facts relevant to the conflict of interest determination. In addition, the Interested Person shall respond to factual questions related to the substance of the transaction or arrangement being considered. After such presentation and response to factual questions, he/she shall leave the meeting during the discussion of, and the vote on, the transaction, arrangement or board or committee action that results in the conflict of interest.

2. The chairperson of the board or committee shall, if appropriate, appoint a disinterested person or committee to investigate alternatives to the proposed transaction, arrangement or board or committee action.
3. After exercising due diligence, the board or committee shall determine by a majority vote of the disinterested board members whether the transaction or arrangement or board or committee action is in PE's best interest and whether the transaction or action is fair and reasonable to the Company.
4. An Interested Person can be counted to make up a quorum for the meeting at which the transaction is decided or the board or committee action is taken but he/she may not vote on the transaction or action. The transaction or action must be approved by a majority of disinterested persons even though the disinterested persons constitute less than a quorum.
5. Records of Proceedings

The minutes of the board and all committees with board-delegated powers shall contain –

- a. The names of the persons who disclosed or otherwise were found to have a Financial Interest in connection with an actual or possible conflict of interest, the nature of the Financial Interest, any action taken to determine whether a conflict of interest was present, and the board's or committee's decision as to whether a conflict of interest in fact existed.
- b. The names of the persons who were present for discussions and votes relating to the transaction, arrangement or action, the content of the discussion, including any alternatives to the proposed transaction, arrangement or action, and a record of any votes taken in connection therewith.

D. Violations of the Conflicts of Interest Policy.

1. If any Personnel fail to complete and file with the Company an annual disclosure statement and annual certification as required by this Policy, such person may be prohibited from attending and participating in board/committee meetings until such time as such documents are completed and filed.
2. If the Board or committee has reasonable cause to believe that Personnel has failed to disclose actual or possible conflicts of interest, it shall inform such person of the basis for such belief and afford the member an opportunity to explain the alleged failure to disclose.

3. If, after hearing the response of the member and making such further investigation as may be warranted in the circumstances, the board or committee determines that the member has in fact failed to disclose an actual or possible conflict of interest, the Board may take appropriate disciplinary and corrective action, which may include removal from the position, subject, in the case of removal of a manager, approval of the Company's members.

Exhibit:

Annual Conflict of Interest Disclosure Statement

ANNUAL CONFLICT OF INTEREST DISCLOSURE STATEMENT

To: Compliance Officer

In answering the questions on this Statement, I have included complete information about myself and, to the best of my knowledge, my immediate family (spouse and children). I understand that a "*material interest*" means (i) a position as an officer, director, employee, consultant, trustee or member of a policy-making committee of an entity; (ii) ownership, investment or other beneficial interest in an entity (other than a 5% or less ownership in a publicly traded company or as a result of investments made through a 401(k) money manager); or (iii) a direct or indirect compensation arrangement. (If you need more space to answer any question, attach an additional page.)

1. Do you or any member of your immediate family have any material interest in any organization or entity that sells goods to, furnishes services to, purchases items or services from or otherwise does business with PE? (Answer yes or no. If yes, please list nature of interest and name of entity. Please keep in mind that payors are considered to purchase services from health care providers.)

YES [] NO []

2. Do you or any member of your immediate family have any material interest in any organization or entity that competes with PE in any way, or which would be able to use inside information about PE to the disadvantage of PE? (Answer yes or no. If yes, please list nature of interest and name of entity).

YES [] NO []

3. During the last twelve months, have you or any member of your immediate family given or accepted any gift, entertainment, use of property or facilities or other favors from any person or entity that has an interest in any business transaction or other matter in which you are or have been, or will be, involved on behalf of PE? (Answer yes or no and if yes, please list: (a) the family member's name and relationship to you (if response relates to family member); (b) the name and address of donor person or entity; (c) the nature and value of the gift, entertainment, etc.; and (d) the date. Note: You need not list business meals or other refreshments or token gifts of a value of less than \$50.00.) YES [] NO []

4. Do you or any member of your immediate family have any other relationship with any entity or concern which presents you with a conflict of interest or which you wish to make known in the interest of full disclosure of possible future conflicts of interest? (Answer yes or no. If yes, please provide details.) YES [] NO []

I agree to inform the Compliance Officer of PE of future changes in the status of my affairs with respect to the areas covered by the above questions and will not enter into situations that might be perceived as a conflict of interest with PE. It is understood that this Statement becomes part of the confidential files of PE to be used only to the extent necessary for the administration and verification of its conflict of interest policy.

Signed: _____ Date: _____

Name: _____

Title/Position: _____

Tab 3 GENERAL COMPLIANCE POLICIES		
3.6 Use of Corporate Assets		
Effective Date: 12/1/04	Last Revision Date: 2/1/07	By: PE

Policy:

Personnel will not use corporate assets for more than incidental personal benefit.

Procedures:

1. All travel and entertainment expenses charged to PE should be reasonable in light of an authorized corporate purpose. As a general matter, the travel expenses of spouses and other family members should not be charged to the Company. Exceptions may be made by the Company on a case by case basis.
2. Travel and entertainment expenses that are unrelated to Company business should never be charged to the Company.
3. Corporate assets should never be converted to personal use without the Company's authorization. Embezzlement is a criminal offense.
4. Use of the Company's computers, facsimile machines, telephones and other electronic equipment and communication systems is permitted for incidental personal matters, as long as such use complies with company policy and does not compromise the individual's ability to fulfill the responsibilities of their position. Company resources and communication systems may not be used for communications that contain or promote any of the following:
 - abusive or objectionable language;
 - information that is illegal or obscene;
 - messages that are likely to result in the loss or damage of the recipient's work or systems;
 - messages that are defamatory;
 - use that interferes with the work of the employee or others;

Personnel have no expectation of privacy for communications and documents sent to, from or stored or reproduced on Company equipment. All such documents and communications are subject to Company review.

5. Use of the Company's equipment, supplies, materials or services for more than incidental personal benefit is prohibited without the Company's authorization.

Tab 3 GENERAL COMPLIANCE POLICIES		
3.7 Limitation on Hiring or Contracting; Compliance Background Investigations		
Effective Date: 12/1/04	Last Revision Date: 2/1/07	By:

Policy:

PE will make reasonable efforts to avoid hiring or delegating substantial discretionary authority to persons whose background includes illegal conduct.

Procedures:

1. All applicants for employment at PE will be required to disclose any criminal convictions or exclusion from any government healthcare program.
2. In addition, PE will conduct reasonable background investigations during the pre-employment and physician credentialing process in connection with all positions that involve discretionary authority, billing/coding responsibilities or that require state licensure. Such background checks will minimally include:
 - a. DHHS/OIG cumulative sanction report. The Cumulative Sanction Report may be accessed on the World Wide Web at IGSNet, the web site of the Federal Inspector General or at the DHHS IG “subpage” located at <http://www/sbaonline.sbc.gov/ignet/internal/hhs/oec.html>. Questions may be directed to: Office of the Inspector General, Office of Enforcement and Compliance, 7500 Security Boulevard, Room N2-01-26, Baltimore, Maryland, 21244, (410) 786-9603.
 - b. Source for state or local criminal background check (i.e., State Bureau of Criminal Apprehension, Bureau of Investigation, local Sheriff’s Department, etc.).
2. PE will not fill such positions or contract with individuals or entities when a reasonable background investigation reveals that they have ever been convicted of a criminal offense related to health care, or are currently listed as debarred or excluded from participation in any government health care programs.
3. If PE learns that a person already employed by or under contract with PE has been convicted of a criminal offense related to health care within the past ten years, or is excluded from participation in any government health care program, the employment or contractual relationship with that person will be immediately terminated, absent mitigating circumstances (such as rehabilitation) determined at the sole discretion of the President following consultation with the Compliance Officer.

Tab 3 GENERAL COMPLIANCE POLICIES		
3.8 New Partnerships & Acquisitions- Due Diligence		
Effective Date: 12/1/04	Last Revision Date: 2/1/07	By: PE

Policy:

New Partnership and acquisition due diligence will include criminal and health care fraud background checks on all potential investors, as well as an investigation of any health care fraud sanctions.

Procedures:

1. PE will perform background checks on potential investors in PE to minimally include:
 - a. DHHS/OIG cumulative sanction report. The Cumulative Sanction Report may be accessed on the World Wide Web at IGSNet, the web site of the Federal Inspector General or at the DHHS IG “subpage” located at <http://www/sbaonline.sbc.gov/ignet/internal/hhs/oec.html>. Questions may be directed to: Office of the Inspector General, Office of Enforcement and Compliance, 7500 Security Boulevard, Room N2-01-26, Baltimore, Maryland, 21244, (410) 786-9603.
 - b. Source for state or local criminal background check (i.e., State Bureau of Criminal Apprehension, Bureau of Investigation, local Sheriff’s Department, etc.).

2. PE will not engage in a transaction (e.g., to co-own an endoscopy center) with a potential investor who:
 - a) Has been convicted of a criminal offense related to healthcare (unless such person or entity has implemented a compliance program as part of an agreement with the federal government); or
 - b) Has been listed by a federal agency as debarred, excluded or otherwise ineligible for federal program participation.

3. PE will require any acquisition target to disclose:
 - a) Whether the target or any of its officers, board members or principals has been convicted of a criminal offense related to healthcare (and, if so, whether the target has implemented a compliance program as part of an agreement with the federal government).
 - b) Whether the target or any of its officers, board members or principals which has been listed by a federal agency as debarred, excluded or otherwise ineligible for federal program participation.

- Any pending investigations by a government agency.
- Any corporate integrity agreement, settlement agreement or consent decree with a government agency.
- Any known violations of applicable law.

Tab 3 GENERAL COMPLIANCE POLICIES		
3.9 Anti-trust Compliance		
Effective Date: 2/1/04	Last Revision Date:	By: PE

Policy:

PE will conduct its activities in compliance with all applicable antitrust laws. PE’s antitrust compliance policy is intended to err on the side of caution in order to avoid even the appearance of impropriety, and in many cases, sets a higher standard than is required by law.

Procedures:

1. PE will compete for business based on the quality and price of its services, not by trying to exclude competitors from the marketplace.
2. The following agreements should nearly always be avoided. Indeed, price fixing and market allocation agreements may be *per se* unlawful, regardless of the surrounding facts or circumstances. Accordingly, Personnel will not, without the approval of the Compliance Office, enter into:
 - any agreement with a competitor regarding fee schedules or discounts;
 - any agreement with a competitor limiting quality or service competition;
 - any agreement with a competitor to “blacklist” or otherwise refuse to deal with a provider, group of providers, provider network or managed care entity;
 - any agreement with a competitor not to bid on a given contract opportunity, respond to a request for proposals or provide a quote to a particular payer;
 - any agreement with a competitor to divide markets, whether through allocation of territories, product lines, classes of payors or any other mechanism;
 - any agreement with a competitor regarding advertising content, frequency, spending or placement; or
 - any agreement not to deal with a particular vendor or to deal with a vendor only at a specific price (except through a legitimate group purchasing organization or cooperative).
3. While information regarding competitors from publicly available documents may be shared, Personnel will not attempt to obtain competitively sensitive information directly from a competitor or its officers, directors or employees. Personnel will also not disclose similar information about PE unless approved in advance by the President. Competitively sensitive information includes:

- Past, present or future fee schedules and reimbursement information
 - Pricing policies or formulae
 - Bids and quotes
 - Discounts
 - Promotions
 - Marketing/advertising plans
 - Strategic plans
4. PE will not participate in fee schedule or managed care rate surveys or similar surveys of competitively sensitive information, unless the data requested is at least three months old, the information is gathered by a non-competitor and all assurances are granted that only aggregated statistics reflecting data from at least five facilities will be distributed to the public or survey participants.
 5. Personnel will not make material misrepresentations regarding PE or its services. Nor will Personnel disparage a competitor or the competitor's services unless the statements are true. Even if such statements are true, they could involve PE in expensive lawsuits. Accordingly, criticizing a competitor's services rarely constitutes a sound business practice and is not advised.

Tab 3 GENERAL COMPLIANCE POLICIES		
3.10 Business Gifts and Courtesies		
Effective Date: 12/1/04	Last Revision Date: 2/1/07	By: PE

Policy:

Under PE policy, business gifts and courtesies may be offered and accepted only in accordance with this policy to avoid allegations of unlawful kickbacks or undue influence over patient choice. This Policy does not apply to personal gifts paid for by an individual (as opposed to the individual's employer) in connection with an appropriate occasion (birthday, wedding, birth, holiday, etc.)

Procedures:

1. **Gifts to Potential Referral Sources.** Personnel will not offer, give or facilitate the giving of gifts to current or potential referral sources for any Center or physicians practicing at a Center that exceed a value of \$100 per item or in annual aggregate, except with the prior approval of the President/CEO.
2. **Gifts Given to Patients.** Aside from items of nominal value (\$10.00 per item and \$50.00 in annual aggregate), Personnel shall not offer, give or facilitate the giving of gifts to Center patients.
3. **Gifts from Vendors.** Personnel should not accept gifts from vendors or vendor representatives valued at more than \$100 per item or in annual aggregate.

Tab 3 GENERAL COMPLIANCE POLICIES		
3.11 Travel, Meals and Entertainment		
Effective Date: 12/1/04	Last Revision Date: 2/1/07	By: PE

Policy:

Meals and entertainment will not be offered or provided to physicians who are an actual or potential referral source to any Center except in accordance with this policy. *See also the Financial Policy Manual for Policy & Procedures on Employee Travel, Entertainment & Expense Reimbursement.*

Procedures:

1. **Meals.**

- a. Meals for Actual and Potential Investors in the Company: The restrictions of this policy do not apply to meals offered to actual and potential investors in PE or the affiliated physician’s professional office, as it may be appropriate for PE to provide meals to foster investment and promote investor relations.

- b. Informational Programs and Meetings Involving PE Personnel: Meals may be offered and provided in connection with business meetings and informational programs involving PE, as long as: (i) Personnel participates in the program or meeting; (ii) the purpose of the program or meeting is of a general educational/scientific nature, to discuss a potential legitimate business arrangement or to convey information regarding a Center; (iii) the meals are modest as judged by local standards; and (iv) the meals occur in a venue and manner conducive to informational communications. In no instance should PE provide a meal for a person who: (i) is not in attendance at the program or meeting; or (ii) has no need for the educational/informational presentation (e.g., maintenance staff, spouses, children and other guests). Meals outside the context of formal educational presentations should not be provided on more than an occasional basis. Personnel should not drop off doughnuts, pizza or deli trays or otherwise provide meals to physician referral sources or their staff to be consumed outside the presence of PE Personnel unless there is a clear educational objective.

- c. Meals at Third Party Educational Conferences and Meetings: PE may provide financial support to the sponsors of educational conferences and meetings (including continuing medical education programs) who in turn may provide meals or receptions for all attendees. PE also may directly provide meals or receptions at such events in compliance with the sponsoring organization’s guidelines. In either of the above situations, the meals or receptions should be modest and conducive to discussion among attendees. Further, the amount of time spent by attendees at the meals or receptions should be clearly subordinate to the amount of time spent at the educational activities of the conference or meeting.

For purposes of this policy, “educational conference or meeting” means any activity, held at an appropriate location, where (a) the gathering is primarily dedicated, in both time and effort, to promoting objective scientific and educational activities and discourse (one or more educational presentation(s) should be the highlight of the gathering), and (b) the main incentive for bringing attendees together is to further their knowledge of the topic(s) presented. Personnel should obtain prior approval from the President/CEO or Compliance Officer before offering to provide or sponsor a meal or reception at a third-party educational conference or meeting.

2. **Entertainment, Travel and Recreational Events.** Although business entertainment is a customary practice in many industries, it may generate significant exposure in the health care industry. Accordingly, Personnel should not provide or offer entertainment, trips or recreational events for current or potential Center referral sources. This includes, but is not limited to resort vacations, boating trips, concerts, golf outings and sporting events, even when in connection with an educational program or a third party conference. The only exceptions are for entertainment, travel and lodging provided (1) to PE consultants and service providers in accordance with Section 3 of this policy; and (2) to actual or potential investors in a Center in which PE holds or is considering an investment interest; and (3) to actual or potential investors in PE.
3. **Consulting and Service Arrangements.** Personnel should not offer compensation for consulting or other services provided by a current or potential referral source to PE, except in connection with an arrangement that satisfies the following criteria:
 - a. There is a written contract specifying the nature of the services to be provided;
 - b. The contract specifies the compensation amount or formula, which must be consistent with the fair market value of the services provided;
 - c. A legitimate need for the services has been clearly identified;
 - d. The criteria for selecting consultants/service providers is directly related to the identified purpose and is not related to the volume or value of PE products ordered, purchased or recommended by the individual;
 - e. The number of consultants/service providers retained is not greater than the number reasonably necessary to achieve the identified purpose; and
 - f. PE maintains records documenting the services provided.

It is appropriate for PE to offer reimbursement for reasonable travel, lodging and meal expenses incurred by an individual while providing services to PE. PE also may provide modest entertainment and recreational activities in connection with meetings involving PE consultants and service providers, provided that (i) the venue and circumstances of such meetings are conducive to the provision of services; (ii) activities related to the services are the primary focus

of the meeting; and (iii) any social or entertainment events are clearly subordinate in terms of time and emphasis. Token consulting or advisory arrangements that involve little if any real work for PE should never be used to justify compensating health care professionals and others in a position to refer or influence referrals to a Center for their time, travel, lodging or out-of-pocket expenses.

Tab 3 GENERAL COMPLIANCE POLICIES		
3.12 Government & Political Interactions		
Effective Date: 12/1/04	Last Revision Date: 2/1/07	By: PE

Policy:

Personnel are free to make their own individual decisions in political matters. However, Personnel will strictly avoid seeking to influence any government employee’s judgment by promises of gifts, loans or any other unlawful inducement.

Procedures:

1. No Personnel should be pressured to participate in political activity or contribute to any political cause or candidate.
2. Personnel are free to become involved in lawful political activities, provided that such activities do not occur on Company time or involve the use of Company property, equipment or supplies, including computers and letterhead. All political activity should be conducted in an individual capacity and not on behalf of the Company.
3. PE does not make corporate political contributions. Therefore, no contributions of Company funds will be permitted in connection with any federal, state or local election. However, the Company may incur expenditures in connection with proper lobbying activity related to Company operations and approved by an Officer.
4. Gifts, loans and other inducements aimed at influencing a government employee’s judgment are strictly prohibited.

Tab 3 GENERAL COMPLIANCE POLICIES		
3.13 Financial Reporting Integrity		
Effective Date: 12/1/04	Last Revision Date: 2/1/04	By: PE

Policy:

PE will exercise due diligence to ensure that transactions are reported accurately in material respects.

Procedures:

1. All funds and other assets and all transactions of the Company must be properly documented, fully accounted for and promptly recorded in conformity with the Company's accounting policies to enable the preparation of timely management reports and to meet external and regulatory reporting requirements. The financial records of the Company must accurately reflect all transactions, including any payment of money, transfer of property or furnishing of services.
 - a. Under no circumstances may Company funds or assets be used for any unlawful purpose.
 - b. Under no circumstances will unrecorded assets or transactions be tolerated, regardless of their intended purpose or use.
 - c. Under no circumstances shall improper, intentionally inaccurate or false entries be made in any of the Company's financial records.

It must be emphasized that an intention to deceive or defraud is not required to constitute a violation of any of these standards. To ensure compliance with these standards, all Personnel are expected to give complete cooperation to PE's finance department and to the Company's independent outside auditors to enable them to perform their duties.

2. Significant deficiencies and material weaknesses in internal controls over financial reporting, as well as any fraud involving management or employees with a significant role in internal controls will be disclosed to PE's auditors and Audit Committee.

Tab 3 GENERAL COMPLIANCE POLICIES		
3.14 Integrity of Data Systems		
Effective Date: 12/1/04	Last Revision Date: 2/1/07	By: PE

Policy:

PE will exercise reasonable care to protect the integrity of its data systems.

Procedures:

In order to protect the integrity of its data systems, PE will:

1. Establish procedures for regularly backing up data.
2. Maintain a complete and accurate audit trail.
3. Maintain systems to prevent data contamination.
4. Perform regularly scheduled virus checks.
5. Maintain mechanisms to protect electronic data from unauthorized access or disclosure.
6. Comply with all applicable laws and regulations regarding electronic data or computer system security and the HIPAA Compliance Policies.

Tab 3 GENERAL COMPLIANCE POLICIES		
3.15 Record Retention		
Effective Date: 12/1/04	Last Revision Date: 2/1/07	By: PE

Policy:

PE will retain records for the applicable required retention period(s) as set forth under federal or state law but in no case less than seven (7) years. Records may only be destroyed in an appropriate manner and after all applicable retention periods have expired.

Procedures:

1. Records shall be kept in their original form or in an acceptable alternate form for storage.
2. Records shall be maintained in a usable condition and in an appropriate environment to ensure the integrity of the information they contain.
3. All records maintained by PE must be legible, appropriately organized and available for audit and review by auditors, both internal and external.
4. The confidentiality of all records pertaining to patient care will be maintained in accordance with federal and state laws and the HIPAA Compliance Policies.

Tab 3 GENERAL COMPLIANCE POLICIES		
3.16 Responding to Government Investigation		
Effective Date: 12/1/04	Last Revision Date: 2/1/07	By: PE

Policy:

PE will appropriately cooperate with government investigations in a manner that protects the Company's best interests.

Procedures:

As healthcare law enforcement has grown more aggressive, the search warrant has become a regular method used by governmental authorities to obtain evidence of alleged healthcare fraud and abuse. Law enforcement officers executing a warrant typically arrive at an office or facility with no prior notice, armed with a search warrant that entitles them to seize original business records, including computer records. Government investigators may also arrive unannounced at the homes of present or former personnel and seek interviews and documentation.

The Board has designated the Compliance Officer as the PE manager in charge during a search warrant event. The Compliance Officer shall contact legal counsel immediately in the event law enforcement officers arrive at PE. The Compliance Officer (and the Board) shall be responsible for coordinating PE's response to a search or request for interviews.

I. First Steps

- A. Identify the lead investigation officer and request:
 - 1. all of the investigating officers' credentials, agency affiliations, business cards, business telephone numbers and addresses;
 - 2. a copy of the search warrant and/or subpoena (if any);
 - 3. if a search, a courtesy delay in initiating their search in order for you to contact legal counsel; and
 - 4. if an interview, that all Personnel be represented by PE counsel and that counsel must be present during any interviews.

- B. Contact legal counsel immediately and fax a copy of the search warrant and/or subpoena to counsel. If counsel can be reached by phone, put counsel directly in touch with the lead investigating officer.

C. Organize the Personnel

1. Gather all personnel and read aloud the Personnel Guide for Government Investigations (Section IV, below) which pertains to personnel's rights and obligations during an investigation.
2. Assign certain personnel to observe the search, write down what is searched or seized, and write down any questions the investigating officers ask. Send all other personnel home.
3. Ensure that no personnel are left alone with an investigating officer, unless requested by the personnel.

II. A Search:

A. **Without a Warrant.** If the officers do not have a search warrant, DO NOT consent to the search, e.g., if the officer asks if you consent or will allow a search, say "no." Contact legal counsel for further advice.

B. **With a Warrant.**

1. *The Law.* If the officers present a search warrant, they have the authority to enter PE's private premises. The officers may search for evidence of criminal activity and seize documents listed in the search warrant and/or subpoena. However, PE may politely request (but cannot insist) that the officers delay the search until legal counsel is contacted and is able to assist in the interpretation of the warrant.
2. *The Compliance Officer should:*
 - a. Request a delay until legal counsel is contacted and is able to assist in interpreting the warrant (either in person or by phone).
 - b. Review the warrant carefully (if possible with assistance of counsel) and determine:
 - i. The areas specified to be searched.
 - ii. The documents specified to be seized.
 - c. Object if the investigating officers search areas/documents not specified in the warrant.
 - i. Inform the lead officer of your objection.
 - ii. Take detailed notes and photographs.

- d. Object to any search of “privileged” documents. Privileged documents are any communications from or to PE’s legal counsel.
 - i. Do not allow the investigating officers to read any privileged documents. A court must determine whether the investigating officers may read the documents.
 - ii. Negotiate a method for protecting privileged documents until there is a court determination. For example:
 - (a) If the privileged documents remain at PE, place the privileged documents in separate boxes.
 - (b) If the privileged documents are taken off premises, place the privileged documents in sealed envelopes/boxes (and sign the seals).
- 3. Ensure that the investigating officers are never left alone on the premises.

III. A Request for an Interview:

- A. **The Law.** Personnel may refuse to grant an interview to the investigating officers and request legal counsel. Even if personnel decide to answer questions, he/she may stop the interview at any time and request legal counsel.
- B. **The Compliance Officer should request that:**
 - 1. The interview be conducted in the presence of an attorney;
 - 2. The interview be conducted during normal business hours;
 - 3. The interview be conducted, if necessary, at another location; and
 - 4. The reason for the interview be disclosed.
- C. **All personnel should notify their supervisor and the Compliance Officer immediately if a government official requests an interview with them.**

IV. Personnel Guide for Government Investigations:

To be read aloud verbatim (or distributed) to all personnel as soon as possible if there is a search.

1. **As you know, the office is being searched by law enforcement officers. I would like to take a moment to inform you of your rights and obligations.**
2. **First, do not obstruct the search. The officers have a legal right to search the premises and to seize what is designated in the warrant as evidence.**
3. **The investigating officers may ask you to grant them an interview. You are free to do so, but you are under no legal obligation to grant them an interview. The search warrant entitles them to search the premises. It does not entitle them to interview any person.**
4. **If you do grant an interview to the investigating officers, you should be aware that anything you say can be used against you in a criminal prosecution or in a civil enforcement proceeding. This is true regardless of whether the officers give you any so-called Miranda warnings.**
5. **If the investigating officers ask any of you to grant them an interview, and you would like to do so but would like corporate counsel to be present at the interview, we will make counsel available for that purpose. Please let me know if that is the case.**

Tab 3 GENERAL COMPLIANCE POLICIES		
3.17 Intellectual Property and Confidential Information		
Effective Date: 12/1/04	Last Revision Date: 2/1/07	By: PE

Policy:

Personnel shall not misappropriate confidential or proprietary information belonging to PE, or any other person or entity. Nor should personnel utilize any publication, document, computer program, information or product in violation of PE's or any other person's or entity's interest in such product (including copyright and other intellectual property interests).

Procedures:

1. Personnel shall not utilize confidential business information obtained from PE or PE's competitors, including price lists, contracts, payer reimbursement, financial statements or other information for their personal interests or in violation of any law or agreement, (including, for example, a covenant not to compete or a prior employment agreement).
2. Personnel will strive to protect the Company's confidential and proprietary information and to prevent inappropriate or unauthorized disclosures. Personnel should always guard against inadvertent disclosures, which may arise in either social conversations or in normal business relations with vendors, Center staff, physicians and potential investors. Confidential information should not be provided to outsiders without first getting the approval from a Company Officer.
3. Copyright laws protect many materials that are used in the course of our work. Audio and videotapes, trade journals, books and magazines are some examples of these materials. Presentation slides, training materials, management models or other materials prepared by outside consultants or organizations may also be copyrighted. **We may not distribute, copy or alter copyrighted materials owned by others without a valid license or other prior permission of the copyright owner or its authorized agent.** It is not always easy to determine if such permission exists, therefore, we should discuss these issues with a Company Officer.
4. It is against our policy to reproduce copyrighted software, documentation or other materials without permission. **Only legitimately purchased, original software may be installed onto a company computer.** Any and all copying of software is restricted to the provisions of the Software License Agreement. Use of unlicensed software not only creates a legal liability for the Company, but also exposes our computers to a higher risk of computer viruses.

Tab 3 GENERAL COMPLIANCE POLICIES		
3.18 E-Mail Security Policy		
Effective Date: 6/1/2011	Last Revision Date:	By: PE

Purpose:

This policy statement provides specific instructions on the ways to secure electronic mail (e-mail) resident on personal computers and servers.

Scope:

The policies apply to Physicians Endoscopy (PE) Personnel and contractors and cover e-mail located on PE personal computers and servers if these systems are under the jurisdiction and/or ownership of PE. The policies apply to stand-alone personal computers as well as those attached to networks.

Policy:

As a productivity enhancement tool, PE encourages the business use of electronic communications (voice mail, e-mail, and fax). Electronic communications systems and all messages generated on or handled by electronic communications systems, including back-up copies, are considered to be the property of PE (“Company Property”), and are not the property of users of the electronic communications services.

Responsibilities:

As defined below, PE groups and staff members responsible for electronic mail security have been designated in order to establish a clear line of authority and responsibility.

1. Information Systems (IS) must establish e-mail security policies and standards and provide technical guidance on e-mail security to all Physicians Endoscopy staff.
2. IS staff must monitor compliance with personal computer security requirements, including hardware, software, and data safeguards. Managers and supervisors must ensure that their staff is in compliance with the personal computer security policy established in this document. IS staff must also provide administrative support and technical guidance to management on matters related to e-mail security.
3. PE managers must ensure that employees under their supervision implement e-mail security measures as defined in this document.

Procedures:

1. **Authorized usage:** PE electronic communications systems generally must be used only for business activities. Incidental personal use is permissible so long as:
 - (a) It does not consume more than a trivial amount of resources.
 - (b) It does not interfere with staff productivity.
 - (c) It does not preempt any business activity.

Personnel may not use PE electronic communications systems for charitable endeavors, private business activities, or amusement/entertainment purposes unless expressly approved by PE management. The use of corporate resources, including electronic communications, should never create either the appearance or the reality of inappropriate use.

2. **Default privileges:** Personnel privileges on electronic communications systems must be assigned so that only those capabilities necessary to perform a job are granted. This approach is widely known as the concept of "need-to-know." For example, end users must not be able to reprogram electronic mail system software.
3. **User separation:** These facilities must be implemented where electronic communications systems provide the ability to separate the activities of different users. For example, electronic mail systems must employ user IDs and associated passwords to isolate the communications of different users. But fax machines that do not have separate mailboxes for different recipients need not support such user separation. All Personnel and authorized contractors have unique usernames and passwords to access the network system.
4. **User accountability:** Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorized user. To do so, exposes the authorized user to responsibility for actions the other party takes with the password. If users need to share computer resident data, they should utilize public directories on local area network servers, and other authorized information-sharing mechanisms. To prevent unauthorized parties from obtaining access to electronic communications, users must choose passwords that are difficult to guess (not a dictionary word, not a personal detail, and not a reflection of work activities for example).
5. **Default protection:** In the interest of email security PE employs an email encryption system. All email sent from PE users is filtered through this system. Email containing Protected Healthcare Information (PHI), financial information or social security numbers is automatically encrypted before it is sent. Additionally, all email sent between PE and its affiliated centers are encrypted. All other email transmissions are NOT encrypted by default. However, all users have the ability to manually encrypt any email communications. The encryption should be used in situations where a user wants to ensure an email gets encrypted regardless of content.

Even with encryption systems in place, great caution must be taken to ensure that the email addresses used in emails are accurate. When sending an email that includes protected information the user should ensure that the email is addressed to the correct parties.

6. **Respecting privacy rights:** Except as otherwise specifically provided, Personnel may not intercept, disclose, or assist in intercepting or disclosing, electronic communications. However, PE also is responsible for servicing and protecting its electronic communications networks. To accomplish this, it is occasionally necessary for IS staff to intercept or disclose, or assist in intercepting or disclosing, electronic communications without notice.
7. **No guaranty of message privacy:** PE does not guarantee the privacy of electronic communications. Personnel should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed, and stored by others. Furthermore, others can access electronic communications in accordance with this policy.

8. **Regular message monitoring:** The content of electronic communications may be monitored and the usage of electronic communications systems will be monitored to support operational, maintenance, auditing, security, and investigative activities. Users should structure their electronic communications in recognition of the fact that PE will from time to time examine the content of electronic communications with or without cause.
9. **Statistical data:** Consistent with generally accepted business practices, PE collects statistical data about electronic communications. As an example, call-detail-reporting information collected by telephone switching systems indicates the numbers dialed, the duration of calls, the time of day when calls are placed, etc. Using such information, Information Systems (IS) staff monitors the use of electronic communications to ensure the ongoing availability and reliability of these systems.
10. **Incidental disclosure:** It may be necessary for IS staff to review the content of an individual employee's communications during the course of problem resolution. IS staff may not review the content of an individual employee's communications out of personal curiosity or at the behest of individuals who have not gone through proper approval channels. Anything found that is of concern by the IS staff will be reported to the employee's Department Head and/or the VP of Human Resources.
11. **Message forwarding:** Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages. PE sensitive information must not be forwarded to any party outside PE without the prior approval of a supervisor or manager. Blanket forwarding of messages to parties outside of PE is prohibited unless the prior permission of senior management has been obtained.
12. **Purging electronic messages:** Messages no longer needed for business purposes must be periodically purged by users from their personal electronic message storage areas. After a certain period electronic messages backed up to a separate data storage media (tape, disk, CD-ROM, etc.) will be automatically deleted by IS staff. This purging only affects backup data and does not affect individual user mailboxes. Users are asked to maintain their own mailboxes and purge old messages that are no longer needed. Not only will this increase storage space, it will also simplify record management and related activities. If PE is involved in a litigation action, all electronic messages pertaining to that litigation will not be deleted until the PE President or his designated representative has communicated that it is legal to do so.
13. Violation of these policies and procedures may subject Personnel or contractors to disciplinary procedures up to and including termination.

Tab 3 GENERAL COMPLIANCE POLICIES		
3.19 Internet Security Policy		
Effective Date: 6/1/2011	Last Revision Date:	By: PE

Purpose:

The purpose of this policy is to establish management direction, procedures, and requirements to ensure the appropriate protection of PE information and equipment via Internet connections.

Scope:

This policy applies to all Personnel, contractors, consultants, temporaries, and other users at PE, including those users affiliated with third parties who access PE computer networks. Throughout this policy, the words "worker" and "user" will be used to collectively refer to all such individuals. The policy also applies to all computer and data communication systems owned by and/or administered by PE.

Policy:

All information travelling over PE computer networks that has not been specifically identified as the property of other parties will be treated as though it is a PE corporate asset. PE prohibits unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information. In addition, it is the policy of PE to protect information belonging to third parties that has been entrusted to PE in confidence, as well as in accordance with applicable contracts and industry standards.

Responsibilities:

As defined below, PE groups and staff members responsible for Internet security have been designated in order to establish a clear line of authority and responsibility.

- a) Information Systems (IS) must establish Internet security policies and standards and provide technical guidance on PC security to all Physicians Endoscopy staff.
- b) IS staff must monitor compliance with Internet security requirements, including hardware, software, and data safeguards. Managers must ensure that their staffs are in compliance with the Internet security policy established in this document. IS staff must also provide administrative support and technical guidance to management on matters related to Internet security.
- c) IS staff must periodically conduct a risk assessment of each production information system they are responsible for to determine both risks and vulnerabilities.
- d) IS staff must check that appropriate security measures are implemented on these systems in a manner consistent with the level of information sensitivity.
- e) IS staff must check that user access controls are defined on these systems in a manner consistent with the need-to-know.
- f) PE information owners must see to it that the sensitivity of data is defined and designated on these systems in a manner consistent with in-house sensitivity classifications.
- g) PE managers must ensure that:

1. Employees under their supervision implement security measures as defined in this document.
2. Employees under their supervision delete sensitive (confidential) data from their disk files when the data is no longer needed or useful.
3. Employees under their supervision who are authorized for remote access are aware of and comply with the policies and procedures outlined in all Physicians Endoscopy documents that address information security.
4. Employees and contractor personnel under their supervision complete the clearance process upon their official termination of employment or contractual agreement.

Introduction:

The resources, services, and interconnectivity available via the Internet all introduce new opportunities and new risks. In response to the risks, this policy describes PE's official policies and procedures regarding Internet security. It applies to all Personnel (employees, contractors, temporaries, etc.) who use the Internet with PE computing or networking resources, as well as those who represent themselves as being connected—in one way or another—with PE.

All Internet users are expected to be familiar with and comply with these policies. Questions should be directed to the Information Systems Department. Violations of these policies can lead to revocation of system privileges and/or disciplinary action, including termination.

Procedures:

1. Information movement:

- a) All software downloaded from non-PE sources via the Internet must be screened with virus detection software prior to being opened or run. Whenever the provider of the software is not trusted, downloaded software should be tested on a stand-alone (not connected to the network) nonproduction machine. If this software contains a virus, worm, or Trojan horse, then the damage will be restricted to the involved machine.
- b) All information taken off the Internet should be considered suspect until confirmed by separate information from another source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.
- c) It is also relatively easy to spoof another user on the Internet. Likewise, contacts made over the Internet should not be trusted with PE information unless a due diligence process has first been performed. This due diligence process applies to the release of any internal PE information (see the following section).
- d) Users must not place Physicians Endoscopy material (software, internal memos, etc.) on any publicly accessible Internet computer that supports anonymous file transfer protocol (FTP) or similar services, unless PE management has first approved the posting of these materials.
- e) In more general terms, PE internal information should not be placed in any location, on machines connected to PE internal networks, or on the Internet, unless the persons who have access to that location have a legitimate need-to-know.
- f) All publicly writable (common/public) directories on PE Internet-connected computers will be reviewed and cleared periodically. This process is necessary to

prevent the anonymous exchange of information inconsistent with PE's business. Users may only store business documents or software in these folders. Users may not store information that is illegal or deemed inappropriate by PE policy. Examples include, but are not limited to, pirated software, purloined passwords, stolen credit card numbers, and inappropriate written or graphic material (i.e., erotica). Users are prohibited from being involved in any way with the exchange of the material described in the last sentence.

2. Information protection:

- a) Wiretapping and message interception are straightforward and frequently encountered on the Internet. Accordingly, PE secret, proprietary, or private information must not be sent over the Internet unless it has first been encrypted by approved methods.
- b) Credit card numbers, telephone calling card numbers, log in passwords, patient information and other parameters that can be used to gain access to goods or services must not be sent over the Internet in readable form. The PGP (pretty good privacy) encryption algorithm, or another algorithm approved by PE must be used to protect these parameters as they traverse the Internet.
- c) PE software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-PE party for any purposes other than business purposes expressly authorized by management.
- d) Exchanges of software and/or data between PE and any third party may not proceed unless a written agreement has first been signed. Such an agreement must specify the terms of the exchange, as well as the ways in which the software and/or data is to be handled and protected.
- e) PE strongly supports strict adherence to software vendors' license agreements. When at work, or when PE computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden.
- f) Likewise, off-hours participation in pirate software websites and similar activities represent a conflict of interest with PE work, and are therefore prohibited. Similarly, reproduction of words posted or otherwise available over the Internet must be done only with the permission of the author/owner.

3. Expectation of privacy:

- a) Personnel using PE information systems and/or the Internet should realize that their communications are not automatically protected from viewing by third parties. Unless encryption is used, staff should not send information over the Internet if they consider it to be private.
- b) At any time and without prior notice, PE management reserves the right to examine e-mail, personal file directories, and other information stored on PE computers. This examination assures compliance with internal policies, supports the performance of internal investigations, and assists with the management of PE information systems.

4. Resource usage:

- a) PE management encourages staff to explore the Internet, but if this exploration is for personal purposes, it should be done on personal, not company, time. Likewise, games, news groups, and other non-business activities must be performed on personal, not company, time.
- b) Use of PE computing resources for these personal purposes is permissible so long as the incremental cost of the usage is negligible, and so long as no business activity is

preempted by the personal use. Extended use of these resources requires prior written approval by a supervisor or manager.

5. Public representations:

- a) Personnel may indicate their affiliation with PE in website discussions, chat sessions, and other offerings on the Internet. This may be done by explicitly adding certain words, or it may be implied, for instance via an e-mail address.
- b) Whenever staff provide an affiliation, they must also clearly indicate that the opinions expressed are their own, and not necessarily those of PE.
- c) All external representations on behalf of the company must first be cleared with the Marketing Department. Additionally, to avoid libel problems, whenever any affiliation with PE is included with an Internet message or posting, "flaming" or similar written attacks are strictly prohibited.
- d) Personnel must not publicly disclose internal PE information via the Internet that may adversely affect PE's customer relations or public image unless the approval of marketing has first been obtained. Such information includes business prospects, confidential information, and the like.
- e) Care must be taken to properly structure comments and questions posted to mailing lists, public news groups, and related public postings on the Internet so as not to inadvertently disclose projects to the competition. If a user is working on an unannounced project, or related confidential PE matters, all related postings must be cleared with one's manager prior to being placed in a public spot on the Internet.

6. Access control:

- a) All users wishing to establish a connection with PE computers via the Internet must adhere to and follow the procedures and requirements detailed on the PE Remote Worker Policy. All remote workers must authenticate themselves via SSL-VPN before gaining access to PE's internal network. This authentication process must be setup in advance with the IS Department.
- b) Unless the prior approval of the IS Department has been obtained, staff may not establish Internet or other external network connections that could allow non-Physicians Endoscopy users to gain access to PE systems and information. These connections include the Internet home pages, FTP servers, BitTorrent Sites, P2P File Sharing sites, and the like.
- c) Likewise, unless approved in advance, users are prohibited from using new or existing Internet connections to establish new business channels. These channels include electronic data interchange (EDI) arrangements, electronic malls with online shopping, online database services, etc.

7. Reporting security problems

- a) If sensitive PE information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, the IS Department must be notified immediately.
- b) If any unauthorized use of PE's information systems has taken place, or is suspected of taking place, the IS Department must likewise be notified immediately. Similarly, whenever passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed, the IS Department must be notified immediately.
- c) Because it may indicate a computer virus infection or similar security problem, all unusual systems behavior, such as missing files, frequent system crashes, misrouted

messages, and the like must also be immediately reported. The specifics of security problems should not be discussed widely but should instead be shared on a need-to-know basis.

- d) Users must not "test the doors" (probe) security mechanisms at either PE or other Internet sites unless they have first obtained permission from the IS Department. If users probe security mechanisms, alarms will be triggered and resources will needlessly be spent tracking the activity.

Tab 3 GENERAL COMPLIANCE POLICIES		
3.20 Remote Access Policy		
Effective Date: 6/1/2011	Last Revision Date:	By: PE

Policy:

PE will implement safeguards and processes regarding remote user access to PE network and information technology systems. This policy only applies to those employees granted access or who have the authority to grant or monitor access. Participation in a remote access program is not extended to every employee. Remote access is meant to be an alternative method of meeting PE needs. Therefore, remote access privileges may not be granted or, if granted, may be terminated at any time.

Procedures and Requirements:

1. **Acceptable Use:** Hardware devices, software programs, and network systems purchased and provided by PE for remote access are to be used only for creating, researching, and processing PE-related materials. By using PE’s hardware, software and network systems you assume personal responsibility for their appropriate use and agree to comply with this policy and other applicable PE policies, as well as City, State and Federal laws and regulations.
2. **Eligibility:** Your eligibility to remotely access PE’s computer network will be determined by your manager. Access will be granted upon completion of a properly authorized Remote Worker Access Request Form.
3. **Equipment & tools:** PE may provide tools and equipment for remotely accessing the corporate computer network. This may include computer hardware, software, e-mail, voicemail, connectivity to host applications, and other applicable equipment as deemed necessary. The use of equipment and software provided by Physicians Endoscopy for remotely accessing PE’s computer network is limited to authorized persons and for purposes relating to PE business. PE will provide for repairs to PE equipment. When the employee uses her/his own equipment, the employee is responsible for maintenance and repair of that equipment.
4. **Use of personal computers and equipment:**
 - a) There are literally thousands of possible interactions between the software needed by the remote user and the average mix of programs on most home computers. Troubleshooting software and hardware conflicts can take hours, and can result in a complete reinstall of operating systems and application software as the only remedy for problems. For that reason the Information Technology department will only provide support for equipment and software provided by PE.
 - b) PE will bear no responsibility if the installation or use of any necessary software causes system lockups, crashes, or complete or partial data loss. The employee is solely responsible for backing up data on their personal machine before beginning any PE work.

- c) At its discretion, PE will disallow remote access for any employee using a personal home computer that proves incapable, *for any reason*, of not working correctly with PE provided software or network systems.

5. Personal computer software requirements: In order to access PE resources from your personal computer, your personal computer is required to have:

- a) Antivirus Software
 - This software must be current with up to date definitions and must be configured to scan files while you use them (commonly called Active Protection)
- b) Anti-Spyware Software
 - This software must be current with up to date definitions. In some cases, Anti-Spyware software is included as part of an Antivirus software package. However, that is not always the case.

This software is the responsibility of the user; PE will not be responsible for providing or maintaining it.

6. Wireless Network requirements:

- a) If you will be accessing PE systems over a private local wireless network (Home Wi-Fi) then that connection must be encrypted. Acceptable encryption standards are WEP, WPA, and WPA2. Most wireless routers purchased within the last few years have the ability to encrypt the wireless signal. It is the employee's responsibility to ensure that their wireless network is secure and encrypted.
- b) If you are accessing PE resources via a public Wi-Fi Network you need to have a software firewall active and running on your computer. Examples of public Wi-Fi networks include Hotspots, Hotel wireless, Airport wireless, coffee shops, etc... Acceptable software firewalls include Microsoft Windows Firewall, Norton Internet Security, Norton 360, McAfee Internet Security, etc... Be aware that simply having anti-virus software does not mean you also have a software firewall. If you are using a computer supplied by PE, the firewall is enabled and supported by the PE IT department. If you are using a personal computer, it is the employee's responsibility to ensure that an acceptable firewall is installed and running.

7. Accessing protected healthcare information (PHI): Accessing protected healthcare information (PHI) requires additional concerns and safeguards. In order to access PHI remotely, you must ensure that all information will be displayed and controlled in such a manner that only people authorized to access it can view it. You must ensure that any PHI is closed or hidden before you leave your computer for any prolonged period of time. You must also agree to abide by all HIPAA regulations that pertain to patient confidentiality as outlined in the PE HIPAA compliance plan.

8. Violations and Penalties: Penalties for violation of this policy and its procedures and requirements will vary depending on the nature and severity of the specific violation. Disciplinary action may include, but is not limited to, reprimand, suspension and/or termination of employment.

Tab 4 GENERAL COMPLIANCE POLICIES		
4.1 Prohibition on Making False Statements on Any Government or Private Document		
Effective Date: 2/1/07	Last Revision Date:	By:

Policy:

PE strictly prohibits the filing of claims that PE knows to include false information with any Federal, state or private payer.

Procedures:

1. Any individual working at or on behalf of PE is prohibited from making false statements or otherwise falsifying information in PE’s books or records and on any document prepared for or filed with any government or private entity or person.
2. In the event that an PE Personnel has reason to believe that billing or claims information received from a physician is false in any respect (whether intentionally or unintentionally), the employee has an obligation to notify his/her manager or the Compliance Officer and to refrain from filing the claim pending further instruction from the Manager or Compliance Officer.
3. Managed centers are obligated by law to bill only for health care services or products that are properly documented. Accordingly, the Centers will be responsible for ensuring that all procedures are properly documented.

Tab 4 GENERAL BILLING POLICIES		
4.2 Ambiguity in Physician Documentation for Billing		

Effective Date: 2/1/07	Last Revision Date:	By:
------------------------	---------------------	-----

Policy:

Whenever documentation of services received from a Center appears to be ambiguous, confusing, conflicting, incomplete or erroneous, the billing staff will contact the Center for clarification or resolution prior to submitting the information for billing.

Background:

The submission of false claims to the government can result in severe criminal and civil penalties. Such penalties can be levied against a Facility that knowingly submits false claims based on erroneous documentation, as well as against the healthcare provider. Further, reasonable diligence must be exercised to preclude the filing of claims based on ambiguous, conflicting, incomplete or erroneous provider documentation.

Procedures:

1. If any PE staff member believes that documentation that will be used for billing is unclear, ambiguous, incomplete, erroneous or conflicting, he/she will notify his/her Manager.
2. The Manager or designee will contact the Center Manager/Administrator and request clarification to ensure that documentation is updated accordingly and within legal guidelines subject, as applicable, to the treating physician's approval.
3. It is expected that the Center physicians will respond to such inquiries in a timely and professional manner.
4. If the codes reflected in the original documentation was already entered into the billing system, any changes are to be communicated to the billing office so that the claim can be corrected and resubmitted.

Tab 4 GENERAL BILLING POLICIES		
4.3 Documentation of Medical Necessity		
Effective Date: 2/1/07	Last Revision Date:	By:

Policy:

PE will not knowingly submit a claim on behalf of a Center when it is known that the services provided were not medically necessary unless there is documentation from the treating physician or an acknowledgement of personal financial responsibility from the patient signed prior to providing any service to the patient. In the case of Medicare beneficiaries, the acknowledgement of personal financial responsibility shall be in the form of an Advance Beneficiary Notice (ABN) obtained in accordance with policy. In the case of non-Medicare beneficiaries, the acknowledgement of personal financial responsibility shall be in the form of a Commercial ABN (a form adapted for use with non-Medicare beneficiaries, but similar to the Medicare ABN form).

Procedures:

1. It is the Center’s responsibility to inform PE if a procedure is not medically necessary and to obtain the appropriate documentation from the patient
2. The Center is responsible for obtaining an ABN for services rendered to a Medicare beneficiary that are not likely to be deemed “reasonable and necessary” by Medicare and billed in accordance with Policy 4.8 Advance Beneficiary Notices. In the case of non-Medicare patients, the center may use a Commercial ABN form to document the same.
3. Nearly all payer contracts are requiring advance written notice to a patient in order to bill a claim denied for medical necessity to the patient. In the event that a facility claim is denied for Medical necessity, PE Billing Personnel will contact the Center Administrator/Manager to obtain evidence of an ABN. In the absence of such written notice, the claim must be written off in accordance with the language in most payer contracts.
4. PE will not bill a payer for items or services that are known not to be medically necessary when the applicable payor contract prohibits the submission of claims for services that are not medically necessary.

Tab 4 GENERAL BILLING POLICIES		
4.4 Upcoding and Unbundling		
Effective Date:	Last Revision Date: 12/31/07	By:

Policy:

PE will report any suspected upcoding, unbundling or any similar billing practices that are intended to improperly increase reimbursement.

Definition:

Upcoding is the practice of billing for services using a code (DRG, CPT or other) that provides a greater reimbursement than would be provided by the billing code assigned to the service actually rendered. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) modified applicable legal requirements to expressly prohibit upcoding. The HIPAA amendments prohibit any “claim for an item or service that is based on a code that the person knows or should know will result in a greater payment to the person than the code the person knows or should know is applicable to the item or service actually provided.”

Example: A physician performs a diagnostic colonoscopy with no additional maneuvers that qualifies to be billed as a 45378. If the physician bills a colonoscopy with snare of polyp (45385), the physician has upcoded.

Unbundling occurs when separate billing codes are used for services that have an aggregate billing code.

Procedures:

1. If PE staff becomes aware that a physician has upcoded or unbundled a particular service(s), the service will not be submitted for billing and a PE Billing Manager/Supervisor will be notified. PE will also contact the Center Administrator/Manager.
2. In addition, if a PE staff member detects a pattern of coding that appears to indicate upcoding or unbundling, the staff member will report the issue to the Compliance Officer for follow-up and review.
3. Personnel will cooperate with any approved billing and coding audits authorized by the Centers. .

Tab 4 GENERAL BILLING POLICIES		
4.5 Responsibility for Coding Updates		
Effective Date: 2/1/04	Last Revision Date:	By:

Policy:

PE will take reasonable steps to ensure that its billing system (e.g. Advantx) is updated to reflect changes in billing codes and rules. PE will monitor changes that may impact coding and billing related to the services provided by Centers that we provide billing services to.

Procedures:

Failure to update coding systems and forms may result in inaccurate claims being filed for patient services. Inaccurate claims may be prosecuted as false claims under federal law.

9. PE will use reasonable care in ensuring that its billing codes (CPT & ICD-9), billing forms, and billing systems (e.g. Advantx) accurately reflect current billing codes and descriptions.
10. To ensure the accuracy and integrity of patient and financial data, PE will designate personnel to ensure that all billing forms, billing codes, coding guidelines and billing programs are updated in a timely manner.
11. All services billed by PE shall be coded in accordance with the current guidelines contained in the Medicare Policy Manuals. PE will use the billing codes as set forth by the current
 - International Classification of Diseases, Clinical Modification (currently in its ninth edition, ICD-9-CM), and
 - Current Procedural Terminology (CPT) coding conventions, and
 - Other relevant guidelines published by the American Medical Association (AMA) or another authoritative agency or organization, in determining proper codes

Tab 4 GENERAL BILLING POLICIES		
4.6 Medicare as a Secondary Payer		
Effective Date: 2/1/07	Last Revision Date:	By:

Policy:

PE will educate billing Personnel on proper identification of primary, secondary and tertiary insurers for services rendered to patients in accordance with Medicare Secondary Payer requirements and this policy.

Background:

Under the Medicare as Secondary Payer provisions of the Social Security Act, Medicare excludes items or services from coverage to the extent that another third party payer bears primary responsibility for payment. Third party payers bearing primary responsibility for payment are required to process and make payment on claims in accordance with the coverage provisions of their contract with or liability to the beneficiary. If the primary (third-party) payer makes payment but a balance remains outstanding, Medicare will reimburse the provider for the remaining balance in accordance with program rules. Medicare will make secondary payment to satisfy a claim's outstanding balance only after the primary payer makes payment.

The following third party payers are typically considered primary payers for health care items or services within the scope of their coverage arrangements with their respective beneficiaries:

1. Group health plans insuring individuals ages 65 or older who are currently employed or whose spouse (of any age) is currently employed;
2. Large group health plans insuring individuals (eligible for Medicare benefits on the basis of their disability) who are either currently employed or whose family member is currently employed;
3. Group health plans insuring individuals who have End Stage Renal Disease (ESRD) during a thirty (30) month period (called the Coordination of Benefits Period), beginning with the first month that the beneficiary is entitled to Medicare;
4. Workers' Compensation plans (including black lung benefit programs and other government payment programs) of the States or the United States;
5. No-fault insurance plans including automobile medical and non-automobile no-fault insurance; and
6. Liability insurance (e.g. automobile liability insurance and malpractice insurance).

Tab 4 GENERAL BILLING POLICIES		
4.7 Inappropriate Balance Billing		
Effective Date: 2/1/07	Last Revision Date:	By:

Policy:

PE acknowledges that the Center’s participation with Medicare Part B and other governmental programs (e.g. Medicaid, Tricare/Champus), as well as agreements with third party payers requires the Center to accept the approved or allowable charge as payment in full (less any applicable co-payments, deductibles and coinsurance). Additionally, Medicare, Medicaid and most third party payer contracts prohibit billing the patient for non-covered services in the absence of advance written notice signed by the patient. Consequently, PE acknowledges that the difference between a Center’s total charges and the allowable amount is considered a contractual allowance and will not bill a patient this balance. Nor will PE bill for non-covered services that are denied by the payer except in accordance with that payer’s rules and regulations.

Procedures:

1. The Medicare program requires that participating suppliers, including facilities, accept the Medicare Part B allowable amount as payment in full for medically necessary covered services rendered to Medicare beneficiaries. It is unlawful to bill a Medicare beneficiary for the difference between the facility’s total charges and the Medicare Part B allowable amount. Such practice is known as inappropriate balance billing.
2. Likewise, the Medicaid program and most payer contracts prohibit health care providers from billing beneficiaries for the difference between the facility’s total charges and the Medicaid or contractually allowable amount.
3. PE will not balance bill any patient who is a beneficiary of a governmental or commercial payer except for co-payments, coinsurance and deductibles as allowed by the payer and as indicated on the Explanation of Benefits.
4. Additionally, PE will not balance bill a patient/beneficiary for denied services unless the patient/beneficiary was notified in advance in writing of that the service was not covered unless allowed by the payer. Many payer contracts specifically prohibit such balance billing without appropriate advance written notice signed by the patient acknowledging such. For Medicare, there are also specific rules governing such - see Policy on Advance Beneficiary Notices (ABN).

Tab 4 GENERAL BILLING POLICIES		
4.8 Advance Beneficiary Notices (ABN)		
Effective Date: 2/1/07	Last Revision Date: 12/31/07	By:

Policy:

PE will educate its Billing Personnel on the Medicare program requirement and any similar payer requirements that specify when a health care provider knows or should know that Medicare or the payer is likely to deny coverage of a service because such service (e.g. procedure) is not “reasonable and necessary”, the provider will notify the beneficiary that the procedure or service is likely not to be covered and to obtain an executed advanced beneficiary notice (“ABN”) before providing the service. Accordingly, PE will not knowingly bill a Medicare or non-governmental beneficiary for a service that would otherwise be covered by Medicare or the payer except for failure to satisfy the “reasonable and necessary” criterion unless a signed ABN is on file or, in the case of non-governmental payers, PE is able to document that this is not required. Many payers are including this language in the facility provider contract in keeping with Medicare ABN rules.

Procedures:

1. Proper Notice Procedures

If the physician documentation indicates that the services are unlikely to be deemed “reasonable and necessary” by Medicare or the payer, then the Center is responsible for obtaining a written ABN from the beneficiary/guarantor (or the beneficiary’s authorized representative) *prior to providing any service to the beneficiary*. **Note: Medicare regulations allow a single ABN to be obtained when one party provides the professional component and another provides the technical component of a service].** The following specific procedures will be followed:

- A. The ABN must be given personally to a Medicare beneficiary or the guarantor before provision of a service that is not “reasonable and necessary” and, therefore, not covered by Medicare or the payer.
- B. The ABN must be, completed in its entirety, and signed by a Center representative.
- C. The ABN must identify a specific service(s) believed to be non-covered and the estimated cost.
- D. The ABN must state the specific reason(s) why the Center believes that the service(s) is not “reasonable and necessary” and, therefore, not covered.
- E. Center Staff must use reasonable efforts to discuss with the beneficiary or guarantor (or the beneficiary’s authorized representative) that his/her options are

to either (1) agree to become personally responsible for the payment of the service if Medicare denies coverage; or (2) refuse the service.

- F. The beneficiary (and the beneficiary's authorized representative) must be provided with the opportunity to request further information and/or assistance in understanding and responding to the ABN, including the basis for the assessment that items or services may not be covered. Center staff will politely and thoroughly respond to all such inquiries.
- G. Center staff must use reasonable efforts to obtain the signature of the beneficiary (or the beneficiary's authorized representative) after notating on the ABN the patient's decision to either refuse treatment or to become personally responsible for payment.
- H. If the patient refuses to sign the ABN, then the ABN should be annotated to indicate the refusal and the circumstances and persons involved. The annotation should be signed by the Center staff member who has discussed the ABN with the beneficiary and witnessed by a second Center staff member. The annotation may be placed either in the margins of the ABN or on the unused patient signature line.
- I. The center will enter a note in the billing system that a properly executed ABN is on file.

Failure to follow the foregoing procedures may result in the ABN being deemed invalid.

2. Genuine Doubt or Actual Knowledge Requirement

ABNs will be provided only when there is a genuine doubt or actual knowledge regarding the coverage of an item or service under Medicare or the applicable payer. PE will not encourage any process that is prohibited by Medicare or that may be prohibited by contractual obligations with payers, including the use of:

- a) "Routine ABNs" (i.e., where there is no specific, identifiable reason to believe that Medicare or the payer will not pay)
- b) "Generic ABNs" (i.e., which do no more than state that denial of payment is possible) or
- c) "Blanket ABNs" (i.e. those that are routinely given to patients regardless of a genuine doubt or actual knowledge that a specific service is non-covered)

4. Billing

When a Medicare beneficiary or other patient executes an ABN indicating that he or she wishes to receive a service with the understanding that Medicare or the payer is unlikely to provide coverage, the claim should still be submitted to Medicare or the primary insurance. If the payer does pay the claim, any payments made by the beneficiary will be

refunded (except applicable co-pays, coinsurance and deductibles). If the claim is denied, the beneficiary will be personally and fully responsible for payment, either out of pocket or through other insurance that the beneficiary may have.

This policy does not apply to items or services that are not covered due to reasons other than failure to satisfy the “reasonable and necessary” criterion.

Tab 4 GENERAL BILLING POLICIES		
4.9 Reviewing Denials, Rejections and Write-offs		
Effective Date: 2/1/07	Last Revision Date:	By:

Policy:

PE will institute a mechanism for tracking denials, rejections and write-offs on a monthly basis through the billing system and report on such to the Centers on a regular basis to determine if any patterns in payor actions suggest that corrective action may be necessary to ensure that billings are consistent with contractual and legal requirements. When such review indicates that a Center may need to correct or modify its coding practices, PE will notify the Center Administrator/Manager to address and take action in accordance with PE's and the Center's Compliance Program.

Procedure:

1. PE policy mandates the exercise of due diligence in conducting medical billing activities in a manner that is consistent with applicable legal and contractual requirements.
2. As one means of testing legal and contractual billing compliance, PE will track denials, rejections and write-offs through the use of identifiable journal codes tracked in the billing system. Often a pattern of denials, requests for additional documentation, rejections or other similar action by a third party payor indicates that some facet of the medical billing activity in question may be in need of adjustment or other corrective action.
3. PE will regularly report to the Center, numbers and amounts of rejections, denials and write-offs so that the Center can determine if any such patterns suggest that adjustment or corrective action may be needed. If necessary, PE will report concerns to the PE Compliance Officer.

Tab 4 GENERAL BILLING POLICIES		
4.10 Waiver of Patient Co-payments, Coinsurance and Deductibles		
Effective Date: 2/1/07	Last Revision Date:	By:

Policy:

PE encourages its affiliated Centers to make reasonable efforts to collect co-payments and deductibles at the time of service and as allowed by the Center’s payer contract. Any adjustments to claims and patient liabilities must be approved by the center and PE is not authorized to waive co-payments, coinsurance, deductibles and other patient liabilities except in accordance with this policy.

Background:

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) amended the Anti-kickback Statute by modifying the definition of illegal “remuneration” to include “waiver of co-insurance and deductible amounts (or any part thereof), and transfer of items or services for free or for other than fair market value”. Courts have interpreted the Anti-kickback Statute as applying if any part of the purpose of an arrangement is to induce referrals. Thus, the waiver of co-payments, coinsurance and deductibles may place PE at risk for civil and criminal sanction under the Anti-kickback Statute.

HIPAA amendments include a new exception to the general prohibition on waivers. Requirements for the available exceptions to the waiver prohibition are set out below in the *Guidelines for Waiver of Co-Payments and Deductibles*. PE will cease collection efforts related to co-payments, coinsurance or deductible amounts only if a waiver is consistent with the *Guidelines*.

Guidelines for Waiver of Co-payments, Coinsurance and Deductibles:

PE will request from the Center authorization to adjust patient liabilities or reduce patient liabilities for any co-payment, coinsurance or deductible amounts (regardless of payer) only if the following three requirements are met:

1. The waiver is not part of an advertisement or solicitation; and
2. The waiver is not routinely offered by the Company; and
3. The waiver satisfies one of the following:
 - a. The waiver is made following the documented good-faith assessment of the patient’s financial need consistent with Center’s Uncompensated Care policy; or
 - b. The waiver is made after failure of documented reasonable efforts to collect the co-payments or deductibles from the patient; or
 - c. PE determines that the waiver is warranted by extraordinary circumstances and the patient is not a Medicare or Medicaid beneficiary.

For the purposes of these guidelines, “reasonable efforts to collect” shall mean the issuance of at least two patient statements over a period of at least 60 days following the date of service or date

of transfer to the guarantor. Any adjustment following this period will be made in accordance with the Transfer to Collection Agency Policy and Adjustment/Bad Debt Policy.

Tab 4 GENERAL BILLING POLICIES		
4.11 Uncompensated Care		
Effective Date: 2/1/07	Last Revision Date:	By:

Policy:

Recognizing that unforeseen financial difficulties occur, many of the Centers that PE provides billing services to are committed to providing uncompensated care to those individuals who have already received services and who can substantiate their inability to pay.

Reference:

Dept. of HHS Poverty Guidelines - see website: <http://aspe.os.dhhs.gov/poverty/03poverty.htm>

Procedures:

1. When a guarantor states that they are unable to pay for the services they have received, PE will:
 - a. Provide a general verbal overview of the Uncompensated Care Policy to the guarantor/patient
 - b. Mail an Application for Uncompensated Services along with a cover letter and self-addressed return envelope to the guarantor/patient; before mailing the application, PE staff will record the Center name, patient name and patient billing account number on the application.
2. In order to be considered for uncompensated care, the guarantor/patient must:
 - a. Complete an Application for Uncompensated Services;
 - b. Sign the application (if married, both must sign); and
 - c. Return the application and required documentation to the Billing Office
3. Uncompensated care may also be provided for patients through agreements with local, federally funded clinics. Such arrangements should be approved by the Center BOM and communicated to the Billing Office.
4. Upon receipt of the completed application, the Billing Office will
 - a. Review the information provided; *Note: Generally, all applications for uncompensated care are deemed approved unless an unusually high income or assets (for example more than \$20,000) are noted on the application. Any questions regarding approval will be referred back to the Center..*
 - b. Mail a letter regarding the status of the applications to the patient
 - c. Update the accounts receivable system accordingly as follows:

- d. Enter comment into patient's account using adjustment form comment (ADJCOM) and enter status of application (i.e. approved or denied)
- e. Record patient information on an Adjustment form and attach the approved uncompensated care application

Tab 4 GENERAL BILLING POLICIES		
4.12 Transfer of Accounts to External Collection Agency and Bad Debt Write-offs		
Effective Date: 2/1/07	Last Revision Date:	By:

Policy:

It is PE’s policy to establish a procedure for the collection of patient accounts through the utilization of an external collection agency or legal firm that specializes in healthcare collections by establishing criteria for accounts receivable follow-up for those accounts that are seriously past due and after all internal collection efforts have been exhausted. Each Center must appropriately authorize the use of an external Collection Agency.

Cross Reference:

Fair Debt Collection Practices Act from the Federal Trade Commission (applies to ALL centers) - see website: www.ftc.gov/os/statutes/fdcpa/fdcpact.htm
 Rosenthal Fair Debt Collection Practices Act (applies to California only) - see website: www.dca.ca.gov/legal/dc_2.pdf

Procedures:

1. Summary of internal collection processes:
 - a. A guarantor receives their first statement within 15 days of the date that the claim is transferred to the guarantor and every 30 days thereafter.
 - b. Each additional statement sent to the same guarantor has a dunning message that gets progressively more demanding. A guarantor receives his/her final internal statement between the 60th and 120th day, depending on Center requirements.
 - c. In addition, the Billing Office will also make periodic phone calls based on the total dollar amount and age of the account as directed by each Center. Payment plans will be arranged and comments will be documented, as appropriate.

2. On or around the first calendar day of every month
 - a. Center will
 - i. Run a Patient Delinquency Report or similar report from the billing system with the specifications as directed by each Center, e.g. “patients that exceed \$51” and “over 90 days outstanding”.
 - ii. Review the Patient Delinquency Report with the physicians at the center.
 - iii. By the 3rd Tuesday of each calendar month, prepare and approve an adjustment form and fax completed form to the Billing Office for any accounts to be adjusted or communicate further instructions to the Billing Office on any account that warrants further internal action.
 - b. The Billing Office will run the same Patient Delinquency Report, check the billing system comments and review the billing ledger (e.g. verifying that there are no unapplied payments).

3. It is important to recognize that once a patient is in collection, the negotiation process must be handled by the external collection agency due to contractual obligations.
4. Collection agencies are chosen based on their collection practices including the ability to understand the uniqueness of medical billing, location, member associations, number of years in business, collection rates and other factors. All collection agencies follow the Fair Debt Collection Practices Act and the California collection agency also follows the Rosenthal Fair Debt Collection Practice. Each Center must approve the use of the External Collection Agency.
5. On a monthly basis, on or around the 3rd Wednesday, patient accounts that match ALL of the Center-approved qualifiers will be sent to the collection agency. The qualifiers typically include accounts meeting a specific dollar balance, days since last payment and/or total days outstanding.
6. All patient balances that meet the criteria above will be written off with the appropriate collection journal code. All accounts that exceed the aging specifications for the center for the number of days outstanding and are less than \$51 will be written off as bad debt.
7. If payments are received on collection accounts either by the Billing Office or at the Center, it is extremely important that the supporting documentation is transmitted to the collection agency as soon as possible so that the collection agency does not continue to pursue the balance and does not negatively affect a patient's credit in error.
 - a. If payments are received at the center, fax copies of payments to the Billing Office immediately upon receipt
 - b. Billing Office will email or fax all copies of payments on collection accounts directly to the collection agency within 24 hours
 - c. Billing Office will adjust the accounts accordingly with the appropriate collection journal codes.
8. The external collection agency will submit to the Billing Office monthly financial reports indicating payments received and the collection agency fee. The Billing Office will update the billing system on a monthly basis to reflect all patient payment activity on the collection agency accounts.
9. PE will monitor the progress of the collection agencies on a regular basis taking appropriate action as needed.

Tab 4 GENERAL BILLING POLICIES		
4.13 Medical Records Release		
Effective Date: 2/1/07	Last Revision Date:	By:

Policy:

It is PE’s policy to ensure that legal requests for medical records are handled in a timely and appropriate manner.

Procedures:

1. If a request for a release of medical records is received by the billing staff through the lockbox, the notice will be immediately faxed, with a corresponding email, to the Center Administrator/Manager.
2. It is the Center’s responsibility to address requests for medical records.
3. Under no circumstances will PE release medical information except as requested by a payer in conjunction with a specific claim and according to the legal obligations stated in the contract between the payer and the Center.
4. Personnel may be asked for a copy of a patient statement or billing claim form related to a legal subpoena of medical records. Documents will only be released to the Center at the Center Administrator/Manager’s request.

Tab 4 GENERAL BILLING POLICIES		
4.14 Fee Schedules		
Effective Date: 2/1/07	Last Revision Date:	By:

Policy:

Each Center will set fees (also referred to as “fee schedule” or “billed charges”) that reflect competitive rates based on existing market conditions in the area and in compliance with all federal and state regulations related to fees for medical services.

Procedures:

1. A single fee schedule will be established and used for all third party insurance payers taking into account Medicare reimbursement rates and market conditions specific to each geographic area.
2. The initial fee schedule will be approved by Center’s Board of Managers
3. Changes to the Fee Schedule (Additions/Deletions of CPTs and Fee Changes) will be submitted in writing, typically via email, to the Billing Office. The Center Treasurer or Administrator will approve the request. Such requests typically are a result of a code selected by the physician which is not already on the fee schedule.
4. Requests for fee changes/deletions/additions will be entered into the appropriate user table in the billing system by the Billing Office within two (2) business days of the receipt of the request or on the applicable effective date indicated, if any. Data must be entered into the:
 - a. Procedure table of the user tables; and
 - b. If insurance contracts are active, the appropriate entry must also be made in the contract file in the billing system.
5. PE will periodically review the fee schedules against current reimbursement methodologies for various payers, current market conditions for a specific geographic location and make recommendations accordingly to the Center Board of Managers. Periodic revisions to the fee schedules must be approved at the Center level according to their required process.
6. PE acknowledges that fee schedules and payer reimbursement should be treated as confidential and not disclosed to external parties.

Tab 4 GENERAL BILLING POLICIES		
4.15 Refunds and Overpayments		
Effective Date: 2/1/07	Last Revision Date:	By:

Policy:

PE will identify and refund overpayments on a timely basis in compliance with any regulatory policies or payer contractual obligations concerning refunds and overpayments. Medicare expects that providers will review all payments in such a manner that all claims not correctly paid will be identified and reported to the Intermediary within 30 days following the close of the calendar quarter in which the credit occurred. PE will, therefore, refund all credit balances or notify the payer within the lesser of a) 30 days following the close of the calendar quarter or, b) the timeframe specified in the payer contract. However, PE will make best efforts to refund or notify the payer no more than 60 days after identifying or learning of an overpayment.

Procedures:

1. Upon receipt of payment in the name of a Center in which the Billing Office:
 - a. Is substantially certain constitutes an overpayment, the Billing Office will generate a request for refund as outlined below.
 - b. Has a question as to whether such payment constitutes an overpayment, the Billing Office will undertake reasonable efforts to address the situation, including, where appropriate, notifying the payer. All correspondence and communications related to obtaining clarification of the refund will be documented. If based upon the payer’s response, the Billing Office is substantially certain that an overpayment has occurred, the Billing Office will generate a request for refund as outlined below.

2. For all identified overpayments, the Billing Office will contact payer and follow their refund process which could include any of the following:
 - a. Payer will process refund by generating an offset to future Center payments.
 - b. Payer will generate a Refund Request letter to Center.
 - c. Payer will request Center to forward the refund to the appropriate department with backup documentation.

3. For all identified overpayments that require a refund check, the Billing Office will generate a Refund Request form. All requests, along with documentation supporting the request for refund will be forwarded regularly to the Center’s Accounts Payable processing staff.

4. PE’s Accounts Payable will process and mail all refund checks to the addressee and record the check number, check date and date mailed on the Request for Refund form. The original will be given back to the Billing Office to post; once posted the original is returned to AP where it will be filed in the AP invoice files under patient refunds.

5. The Billing Office will enter the information into the A/R system using refund transaction codes (RF Codes) for audit/tracking purposes.

TAB 5

OVERVIEW OF RELEVANT LAWS

The PE Compliance Program has been established to help make certain that PE Personnel understand and comply with the laws that affect their work at or on behalf of PE. These laws come in three forms: statutes, regulations and rules. While statutory law carries the greatest weight of authority, rules and regulations are often the place where laws are explained and applied. For this reason, many of PE's compliance policies are based on rules and regulations, especially those that regard billing for health care services. In many cases, the underlying laws are not specifically referenced or cited in PE compliance policies. The following paragraphs provide a brief overview of the laws that have the greatest relevance to PE's Compliance Program, other than specific billing and coding regulations, which will be separately covered with billing and coding staff during compliance training.

Laws that Prohibit Kickbacks, Self-Referrals and Fee Splitting

1. **“Medicare/Medicaid Anti-Kickback Law.” 42 U.S.C. § 1320a-7b(b).** The Anti-Kickback Law prohibits knowingly and willfully offering, accepting, soliciting or receiving any remuneration (including any kickback, bribe or rebate), directly or indirectly, overtly or covertly, in cash or in kind for
 - a. referring an individual for a service that is paid for by a state or federal healthcare program (for example, Medicare and Medicaid); or
 - b. purchasing, leasing, ordering, arranging for, or recommending the purchase, lease, or order of any good, facility, service, or item that is paid for by a federal healthcare program.

Criminal penalties for violation of the Anti-Kickback Law include a fine of not more than \$25,000 or imprisonment for up to five years, or both. The civil penalty for violation is a fine of up to \$50,000 per incident. Violators are also subject to exclusion from federal health care programs. Exclusion means that a provider can no longer participate in or receive payment from the federal health care programs. For example, an excluded physician practice may not bill Medicare for services rendered to Medicare beneficiaries. Individuals can also be excluded from participation. The federal government's compliance program guidance requires that providers take reasonable steps to avoid employing or contracting with any individual who has been excluded.

2. **The Stark Law (Physician Self-Referral Prohibition). 42 U.S.C. § 1395nn.** The Stark Law generally prohibits a physician from referring a state or federal health care program patient for “designated health services” (including physical therapy services) that are provided by an entity with which that physician or a member of the physician's immediate family has a financial relationship (i.e., a compensation

arrangement or investment interest), unless an exception applies. There is an exception for referrals to an ambulatory surgical center when the services provided to the patient are reimbursed under a composite rate. There also is an exception for “in-office ancillary services” that are provided by or under the supervision of a group practice physician, within the same building as a group office or a “centralized location” occupied on a full time basis by the group and billed under a group billing number.

A physician who violates the Stark Law may face penalties including denial of payment for the designated health services, refunds of amounts collected in violation of the Law, and a civil money penalty of up to \$15,000 per claim. Physicians who enter into arrangements or schemes intended to circumvent the Stark Laws may be subject to civil money penalties of up to \$100,000 for each arrangement or scheme. Violators are also subject to exclusion from federal health care programs.

3. **State Self-Referral Bans.** Many states have laws prohibiting physicians from referring patients for health services to an entity in which the health care worker is an investor. Some states follow the Stark Act model by also prohibiting referrals to any entity with which the physician has a compensation arrangement. State self-referral bans typically apply to all payors, not just governmental payors, and some apply to all health care services, not just certain “designated health services.” Many have exceptions for in-office services performed or supervised by a member of the referring physician’s group practice or for situations where the physician directly provides health services within the entity and will be personally involved in the provision of care to the referred patient. Unlike the Stark Act, many state statutes do not have an exception for ASC referrals.
4. **State Fee Splitting Prohibitions.** Many states have laws prohibiting physicians from dividing with anyone other than another physician in a group practice any fee, commission, rebate or other form of compensation for any professional services not actually and personally rendered. Some states only bar fee splitting in return for referrals; others prohibit any percentage of revenue or other arrangement that divides professional fees. Physicians who violate these statutes are subject to discipline. Sanctions may include license revocation and monetary fines.

Laws that Prohibit False Claims and Related Enforcement Statutes

1. **Federal False Claims Act. 31 U.S.C. § 3808.** The Federal False Claims Act prohibits a person from knowingly presenting or causing to be presented a false or fraudulent claim for payment (including making a false record or statement in support of a claim) to the United States Government. No proof of specific intent is required—reckless or negligent presentment of claims is enough to support a finding that this statute has been violated. The False Claims Act is the primary law used by the federal government to prosecute fraudulent health care billing. The maximum penalty for violating the civil False Claims Act is treble damages (three times what the government incorrectly paid) plus a civil fine of between \$5,500 and \$11,000.

2. **False Statements under the Social Security Act: Criminal. 42 U.S.C. § 1320(a)-7b(a); (c).** Under this statute, it is a felony to knowingly and willfully make or cause to be made any false statement of a material fact in any application for payment (including claims for payment for health care services), or for use in determining rights to such payment, under a federal healthcare program.

This statute also makes the following acts criminal offenses:

- a. Concealing or failing to disclose a known occurrence or event that affects initial or continued right to benefits or payments, with an intent to fraudulently secure such benefit or payment either in a greater amount or quantity than is due, or when no benefit or payment is authorized, is also a criminal offense under this statute.
- b. Applying for benefits or payments for the use or benefit of another and, having received such benefit, knowingly and willfully converting the benefit or payment to a use other than for the use and benefit of such other person.
- c. Presenting or causing to be presented claims for physician's services when the individual providing the services was not a licensed physician.
- d. Providing false information in support of an application for enrollment by any Part A providers, or any Part B suppliers, of health care services.

Each violation of these criminal provisions in connection with furnishing items or services that are paid for by a federal health care program is a felony that is punishable by a fine of up to \$25,000, and/or imprisonment of up to 5 years. Violations not related to furnishing items or services are misdemeanors and are punishable by a fine of up to \$10,000 or imprisonment of up to one year or both.

3. **False Statements under the Social Security Act: Civil. 42 U.S.C. § 1320a-7a(a).** This statute prohibits filing any of the following:

- a. a claim for a medical item or service that the person knows or should know was not provided as claimed;
- b. a claim for a Medicare item or service that the person knows or should know is false or fraudulent; or
- c. a claim presented for a physician's service by a person who knows or should know that the provider was unlicensed, or is licensed but such license was obtained through misrepresentation.

Penalties for violating this statute include treble damages (three times the amount the government incorrectly paid) plus up to \$10,000 for each false claim.

4. **General Healthcare Fraud Offense. 18 U.S.C. § 1347.** This statute provides that it is a crime to knowingly and willfully execute or attempt to execute any scheme to defraud any federal healthcare benefits program; or to 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 federal healthcare benefits program.

Penalties for violation of this statute include fines and/or imprisonment. The length of the imprisonment and amount of the fine depends on the result of the violation. If the violation results in death, for example, the violator may be imprisoned for life. In addition, individuals convicted of a healthcare offense may be required to forfeit any property derived from proceeds traceable to the offense.

5. **Mail and Wire Fraud. 18 U.S.C. § 1341.** This statute prohibits the use of mail, wire, radio or television to execute any scheme or artifice to defraud or obtain money or property by means of false or fraudulent representations. These statutes are commonly used to prosecute healthcare providers who submit claims for services that were never rendered, were not rendered as claimed, or that otherwise violate one or more of the healthcare program rules that are explained in PE Compliance Policies.

Violation of these statutory provisions is punishable by a fine of up to \$1,000 and/or up to five years imprisonment for each violation.

6. **False Claims to Insurance Companies. 18 U.S.C. § 1035.** This statute makes it a crime to knowingly and willfully falsify, conceal or cover up a material fact, in any matter involving a public *or private* health care benefit program. Likewise, it is a crime to make any materially false, fictitious or fraudulent statement or representation or make or use any materially false document in connection with the delivery of or payment for health care benefits, items or services under a public *or private* health care benefit program. Violations of these provisions are punishable by fines and/or a prison term of up to five years.

7. **State False Claims Acts.** Many states have false claims acts that bar the knowing submission of false claims to Medicaid (or other state health programs) and/or commercial payers.