
# Compliance Plan

# Table of Contents

# Overview

At ProMedica Health System, Inc. and its subsidiaries ("ProMedica"), we are proud of the values that drive our success. These values shape an environment and culture that nurtures the highest standards in business ethics and personal integrity. These same ethics and values are displayed in our commitment to excellence in the services we provide. We have reached an exemplary level of corporate citizenship that is a benchmark within health care. It is imperative that as individuals we understand and adhere to these principles and values to protect ProMedica's integrity and welfare. To that end, ProMedica has established a Corporate Compliance Plan ("the Plan") that outlines our ethical commitment via our Standards of Conduct as well as our legal and regulatory requirements for select issues covered under the Plan. Healthcare is one of the most highly regulated industries in the country and there are numerous laws and regulations not addressed herein. That does not mean they are not important to ProMedica, but that they are addressed elsewhere within the organization.

## Why do we need a Compliance Plan?

The most important reason for implementing a Compliance Plan is simply because it is the right thing to do. As noted above, we operate in one of the most highly regulated industries in the world. These regulations change frequently and come from numerous sources. Ensuring that we remain in compliance requires a team effort and a mechanism for inquiries/reporting, investigating, and resolving potential issues. It is the intent of the compliance plan to facilitate that process. We also consider compliance with regulations to be a subset of our objective of maintaining the highest standards of moral and ethical conduct. Everyone in the organization has a role in that objective and an affirmative duty to report suspected non-compliance with our standards.

In addition, failure to comply with governmental regulations can result in significant civil and/or criminal penalties for the organization and potentially its employees, officers, directors and agents as well. The severity of the penalties assessed is not necessarily dependent on the dollar value of the disputed issue, or the position of the person within the organization where the noncompliance occurred. For example, civil penalties under the False Claims Act can include fines of up to $11,000 per each "false claim" submitted, and more importantly, the loss of certification to serve Medicare and Medicaid patients. The presence of an effective compliance plan helps to identify potential issues, aids in mitigating risk, and provides a defense if we were to be challenged regarding any of our areas of operation. It may also serve to significantly reduce potential civil and/or criminal penalties.

## What is covered by our Compliance Plan?

Although it is imperative that ProMedica comply with all federal and state statutes, a compliance program too broad in nature will be ineffective. An effective compliance plan will be one that will address the issues most critical to ProMedica, with the flexibility to add additional areas of concern. Areas currently considered most critical include (click on the links to take you to the definition section):

- Standards of Conduct – ethical standards for acceptable behavior
- False Claims – billing & coding regulations supported by patient care documentation

- Medicare and Medicaid Anti-kickback Statutes – prohibition of offering/receiving inducements for referrals
- Health Insurance Portability & Accountability Act (HIPAA) – patient privacy rights and electronic security standards
- Stark I, II & III – physician self-referral laws
- Tax Exempt Standards – requires all transactions with 'disqualified persons' be at Fair Market Value
- Fraud – intentional misrepresentations of material facts leading to harm
- The Fair and Accurate Credit Transaction Act of 2003 (FACTA) – standards for the prevention of identity theft

## Compliance Plan Content

An overview of the ProMedica Compliance Plan is available in policy SP-1.09. There are seven elements the government recommends for a compliance plan to be considered effective. These elements will be expanded upon below, along with the relevant standards under each and include (click on the links to take you to that section):

- Organizational Structure
  - Compliance Officer is Vivien Townsend (419-291-6707) and Compliance Director is Stella Wohlgamuth (419-291-6706)
  - Local Compliance Liaisons and Privacy Officers are available for all business units. A list is available here.
- Policies & Standards
  - See the Definitions section for a description of the Standards of Conduct and Laws/Regulations covered under the Plan.
  - See the section below for relevant standards related to the covered elements and references to applicable policies.
- Auditing & Monitoring
  - Auditing is performed by independent groups both internal and external to ProMedica.
  - Monitoring is performed by those responsible for given processes to ensure compliance in their areas of responsibility.
- Training
  - All new employees receive basic compliance training through new employee orientation.
  - All employees receive annual compliance training through required on-line programs.
  - Management is responsible for ensuring employees under their responsibility are familiar with the compliance issues impacting them and communicating compliance updates/education received as appropriate.
  - The Compliance Dept. provides general education through updates to leadership (with the assistance of the Compliance Liaison Officers), newsletter articles, the Compliance & Privacy webpage on *my*ProMedica, and other means.
  - The Education Sub-Committee of the Compliance and Privacy Council is charged with the evaluation of compliance education needs for the system and the development of content to meet the identified needs.

- Reporting
  - All employees have an affirmative duty and responsibility to report perceived misconduct, including actual or potential violations of laws, regulations, policies, procedures, or the Standards of Conduct.
  - Anyone who submits a good faith report of a suspected non-compliance is protected from retaliation by both law and ProMedica Policy (see Policy SP – 1.13)
  - Reporting should be through the appropriate chain of command.
    - Alternatives include:
      - Calling the Compliance Dept. directly (419-291-0230)
      - Calling the local Compliance Liaison – see list.
      - Calling the anonymous Compliance Hotline (419-824-1815) or (800-807-2693)
- Discipline
  - Any employee (regardless of position) may be subject to discipline, up to and including termination, if it is determined that his/her actions (or inactions) constituted a willful violation of law or a willful failure to adhere to ProMedica's compliance standards.
  - Decisions regarding discipline are coordinated with Human Resources and will follow those policies.
- Remediation
  - The regulations require that we self-disclose certain errors we discover and refund identified overpayments, or we can be held accountable for intentional fraud.
  - The regulations limit response time to 60 days after the issue is identified, so timely reporting of errors is critical.

## Questions:

There is a common Questions & Answers section attached to this document as well as a flowchart of how to report a compliance concern.

Any other questions can be directed to your local Compliance Liaison Officer (see the attached list), the ProMedica Compliance Department at 419-291-0230, or directly to the Compliance Officer or Director as noted above.

## Summary:

Compliance is everyone's responsibility. Ignorance of the rules is not a defense for non-compliance in the eyes of the government. The rules are widely published and available, we have a responsibility to understand and follow them to the best of our ability. Only with the commitment of all ProMedica personnel and affiliates can we ensure our compliance with the myriad of laws and regulations that impact us. Please share you commitment with those around you and don't hesitate to contact the appropriate people with questions – they are there to assist you with understanding the rules and providing guidance on their implementation.

# Definitions

## Standards of Conduct

The ProMedica Standards of Conduct are an internally developed set of principles that guide how we do business. Our values of appropriate conduct in business provide a set of ethical guidelines that outline how we strive to 'do the right thing' for its own sake in addition to strict compliance with laws and regulations.

## False Claims

The False Claims Act (FCA) includes both civil and criminal provisions used in enforcement of the law, which makes it an offense for any person/entity to present a false claim to the Unites States government. The elements necessary to establish a civil FCA violation are (1) presentation of a claim, (2) to the United States government or any program funded by the government, (3) with actual knowledge that the claim is false/fraudulent or with reckless disregard or deliberate ignorance of the truth or falsity of the claim.

## Medicare and Medicaid Anti-kickback Statutes

Makes it a crime for a person (i.e. a physician) to knowingly and willfully solicit or accept payment (or other remuneration) for referring a patient to another person/entity for the furnishing of any item or service for which payment may be made (in whole or in part) by the Medicare or Medicaid programs. The statute also makes it a crime to knowingly and willfully offer or pay remuneration to "induce" such a referral. An "inducement" is any act intended "to exercise influence over the reason or judgment of another in an effort to cause the referral or program-related business."

## Health Insurance Portability & Accountability Act (HIPAA)

Also known as Administrative Simplification, HIPAA details and provides for the enforcement of patient's privacy rights and standards for the electronic transmission of healthcare data. The legislation is sub-divided into four categories:

- Transaction standards for the transmission of claims, enrollment, eligibility, premium payments, claim status, referrals, and the coordination of benefits.
- Code set standards for diagnosis codes, medical procedure codes, national drug codes, and dental procedure codes.
- Privacy standards that require all individually identifiable health information be kept private and not disclosed without the patient's permission.
- Security standards that require processes be implemented to ensure data integrity, confidentiality, and availability.

Transaction and privacy standards were made final and full compliance was required by October 2002 & April 2003 respectively. Penalties for wrongful disclosure of individually identifiable health information can range up to $1,500,000 and 10 years in prison. Compliance with these standards requires ongoing review of operational policies and procedures throughout the organization. Everyone at all levels needs to be familiar with the impact of these standards on their daily activities.

## Stark I, II & III

Prohibits physicians from referring Medicare and Medicaid patients to a hospital or other entity for the provision of "designated health services" if the physician or immediate family member has a financial relationship with that entity, unless an exception exists. Financial relationships are defined as both ownership/investment interests and compensation relationships. Designated health services include physical, occupational, and speech therapy, clinical laboratory services, radiology services (including MRI, CAT scans, and ultrasound services), radiation therapy, durable medical equipment, orthotics and prosthetic devices, home health services, Parenteral and enteral nutrients and supplies, outpatient prescription drugs, and inpatient and outpatient hospital services.

## Tax Exempt Standards

All 501(c)(3) non-profit organizations may not pay more than "reasonable" compensation to a private individual or entity from which it purchases services or items. Likewise, it may not provide items or services for less than fair market value. If these rules are violated, ProMedica could lose its tax-exempt status and/or the I.R.S. may impose a monetary penalty on the persons responsible.

## Fraud

Fraud is defined as an intentional false representation or concealment of a material fact intended to induce another to act in a particular way, resulting in his or her injury. In healthcare this can take the form of a pattern of false claims (see FCA section above) or a financial fraud that is not unique to healthcare such as embezzlement.

## The Fair and Accurate Credit Transaction Act of 2003 (FACTA)

The purpose of this law as it applies to healthcare is to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account. ProMedica strives to prevent the intentional or inadvertent misuse of patient names, identities, and medical records; to report criminal activity relating to identity theft and theft of services to appropriate authorities; and to take steps to correct and/or prevent further harm to any person whose name or other identifying information is used unlawfully or inappropriately.

# Organizational Structure

## Objective:

Compliance plans need to have an established structure in order to ensure proper oversight responsibilities at the appropriate level within the organization and to ensure communication of issues through proper channels.

## The framework:

The ProMedica Compliance Plan has the following primary components:

### The Audit/Compliance Committee of the ProMedica Board

A primary objective of the Audit & Compliance Committee is to ensure that management is taking appropriate action to maintain internal controls and to comply with applicable laws and regulations via oversight of the internal audit function. The committee also monitors the activity of the ProMedica compliance plan to ensure its effectiveness as defined by the Department of Health and Human Services, Office of Inspector General (OIG), and Centers for Medicare & Medicaid Services (CMS), and to detect areas of significant compliance risk.

### The Compliance Council

The compliance committee will meet at least annually and on an ad hoc basis, to address the adequacy of the plan coverage and significant compliance issues as they arise. The committee will consist of ProMedica Executive Leadership and the Vice President, Audit & Compliance. Other individuals may be added as deemed appropriate.

### The Chief Compliance Officer

The Vice President of Audit & Compliance/Chief Compliance Officer is responsible for managing and maintaining the plan. She reports to the Compliance Council at least annually, and to the Audit & Compliance Committee of the ProMedica Board of Trustees semi-annually, or as needed.

The duties of the Chief Compliance Officer include:

- Ongoing assessment of compliance risk to the organization
- Review and monitor adherence to the ProMedica Compliance Program
- Developing or assisting management in the development of appropriate policies and training programs under the plan.
- Monitoring via oversight of internal compliance audits.
- Working with management and others to investigate questions of non-compliance and determining corrective action plans, as appropriate.
- Serve as a channel of communication to receive and direct compliance issues for investigation and resolution
- Monitor regulatory changes, industry trends and issues

### The Director of Compliance

The Director of Compliance shares many of the duties of the Chief Compliance Officer and is a primary contact for the daily operations of the Compliance Plan. She also oversees the Compliance Department activities which include:

- Assessment of organization compliance educational needs
- Serve as a resource for compliance research and guidance
- Investigating reports of suspected non-compliance and ensuring corrective action is taken (as appropriate)
- Monitor and manage the ProMedica compliance hotline

### The Compliance and Privacy Liaison Council

The Compliance and Privacy Council will meet at least quarterly and will consist of each business unit's Compliance Liaison, a Legal department representative, selected functional specialists, the business unit Privacy Officers, and the Director of Compliance and/or the Vice President of Audit & Compliance. The role of the Council is to address implementation issues across the system and aid in communication.

### The Compliance Liaisons

Each business unit has designated a Compliance Liaison. The Liaisons are the primary contacts for compliance questions in each business unit. They comprise the Compliance Council and ensure implementation of action plans to address compliance issues as they relate to their respective business units. The Compliance Liaisons are supported by the Director of Compliance and/or the Vice President of Audit & Compliance, as needed.

## Primary Contacts:

A full list of compliance contacts including the business unit Compliance Liaisons and Privacy Officers is attached to this document. System-level key contacts include:

| | | |
|---|---|---|
| ***Compliance Officer*** | ***Vivien Townsend*** | ***419-291-6707*** |
| ***Compliance Director*** | ***Stella Wohlgamuth*** | ***419-291-6706*** |
| ***Compliance Dept. – Assistant*** | ***Sheree St. John*** | ***419-291-0230*** |
| ***Compliance Hotline*** | ***Local #*** | ***419-824-1815*** |
| ***Compliance Hotline*** | ***Long-distance #*** | ***800-807-2693*** |

# Policies & Standards

## Objective:

The purpose of the Compliance Plan's policies & standards is to define areas of law/regulation covered by plan and the related ProMedica standards under those rules as well as to provide guidance in addressing compliance issues/situations.

See the definitions section for the laws & regulations under which the below standards are defined and referenced.

## Standards of Conduct

At ProMedica, we are proud of the values that drive our success. These values shape an environment and culture that nurtures the highest standards in business ethics and personal integrity. These same ethics and values are displayed in our commitment to excellence in the services we provide. It is imperative that as individuals we understand and adhere to these principles and values to protect ProMedica's integrity and welfare.

Exactly what constitutes an unethical business practice is both a moral and legal question. ProMedica recognizes and respects the right of each person to engage in activities that are private in nature and do not in any way conflict with or reflect poorly on ProMedica. ProMedica reserves the right, however, to determine when any activity represents a conflict with ProMedica's interest and to take whatever action is necessary to resolve the situation. All persons covered by our standards are required to disclose any activities, associations or interests that may conflict with this policy in an effort to resolve the situation(s) in an effective, timely manner that is in the best interest of ProMedica.

The types of issues addressed through the ProMedica Standards of Conduct (SOC) include, but are not limited to:

- Compliance with Laws & Regulations
- Improper Influence
- Acceptance of Gifts and other Benefits
- Speeches, Presentations and Publications (Honoraria)
- Outside Employment and Business Activities/Consulting
- Conflicts of Interest
- Confidential Information and Trade Secrets
- Campaign And Election Guidelines

The Administrative policy defines how the Standards will be communicated, monitored and enforced, while the Standards themselves are defined for three primary groups of Board Members, Employees, and Physicians (employed and non-employed). Board members, salaried employees and employed physicians recertify their compliance with their respective standards annually. Completion of a SOC Certification statement is a condition of employment and a requirement for board membership.

### Examples:

Conflict of Interest:

A member of leadership at a ProMedica facility, also sitting on a board sub-committee for the Mercy System would be considered a conflict of interest since both roles are positions of influence, which would require divided loyalties and opportunities for disclosure of confidential information. Conversely, a nurse working on a per diem basis at both TH and UTMC is acceptable, since these are not positions of influence.

Acceptance and Giving of Gifts:

If supplier offers to cover the hotel and registration costs of a nursing supervisor to attend a training conference, this could be considered a violation of the SOC. One must consider the reason for the vendor's offer. Is it to influence ProMedica's decision making in their favor regarding current or future purchases from the vendor? Is there a real value to ProMedica from the knowledge to be gained by accepting the offer? The business unit presidents/corporate vice-presidents will make that determination. If the nursing supervisor submits the facts of the situation to the appropriate president/VP in advance of accepting the offer and receives written approval from him/her prior to the event, then the SOC are not violated. However, s/he will still need to disclose the trip and who approved it on his/her annual SOC Certification.

While the acceptance of gifts is a SOC issue as outlined above, the offering of gifts to patients could be a violation of the Social Security Act and gifts to others are governed by IRS regulations. Offering any gifts or remuneration to patients (regardless of their financial class/insurance carrier) could be considered an inducement under the Act and is prohibited. Remuneration includes gifts of cash (or equivalents) in any amount, non-routine waiver of copays/deductibles, and transferring expensive goods or services for free or other than fair market value (expensive gifts or services are defined as anything with a value of more than $10 individually or more than $50 in aggregate on an annual basis). There are limited allowed exceptions under these rules. See the Gifts to Patients Policy for details.

Gifts to others such as employees, board members, physicians, and vendors are governed by the Finance Policy CP-2.05. Generally all such gifts should be below $75 in value and must be reimbursed via Accounts Payable process (vs. T&E Reimbursement forms). For employees, these must be non-cash and should be infrequent for special recognition, family crisis, etc. Gifts to board members, physicians, vendors, or their families must not be for the purpose of influencing their behavior directly or indirectly in respect to ProMedica or business dealings therewith.

Honoraria:

Given a scenario where an employee works for several months on a project, which results in a process redesign and substantial cost savings for ProMedica, others in the industry may hear about it and want the employee to present the findings and results at a conference. The employee may also wish to publish it in a trade journal. No proprietary information may be disclosed without proper prior approval. The Employee Standards contain a table of the specific

approvals that are needed depending on the content of the materials. Typically in an example like this, the materials would need to be shared with the appropriate Executive and the Legal Dept. for formal prior approval.

Outside Employment:
If, for example, a Director of Rehab wanted to start a private business providing rehabilitation services, this could be considered a conflict of interest since it would be in competition with ProMedica and, given the Director's role in provision of those services at ProMedica, there would be opportunities for diversion, etc. If however, that same Director's private business was selling collectables online (or other non-medical industry business) that would not be a concern under the standards as long as it is conducted on an individual's own time.

## Proper Billing & Charging

The appropriate billing of our services is not solely an issue for the Billing Department. Ensuring the accuracy of the claims submitted for the services we provide begins with the moment a patient arrives for admission/registration and is dependent on each step of the patient's experience though the process, including documentation of care, proper coding, and billing. We can provide the best quality of care, but if we do not properly document that care in a manner that supports our charges or we routinely submit claims in error, that can lead to significant fines and penalties that could negatively impact our ability to receive reimbursement and provide those services in the future.

### Standards:

- All billing will be consistent with Medicare/Medicaid rules.
- All documentation will accurately reflect the patient's condition, medical treatment, and procedure provided.
- All coding will accurately reflect procedures performed or diagnosis as documented.
- All charges will be substantiated with physician orders, medical necessity, and with medical services provided.
- Claim submission will adhere to all applicable Medicare/Medicaid rules and government regulations.
- Cost reports will be completed according to Medicare/Medicaid rules and regulations.

Standards specific to the use of Electronic Medical Records (EMR) include:

- Providers should refrain from copy/pasting documentation from a prior note or record, since this practice leads to the appearance of duplicate or "cloned" documentation.
- Copying and pasting documentation from one author to another is prohibited without citation of the original author.
- Providers are encouraged to cite and summarize relevant portions of a patient history, progress note, lab, pathology, radiology results, etc., rather than copying such data into a new medical record entry.

## Policies:

In addition to professional standards for the various disciplines across our organization, there are a variety of policies at the corporate level as well as each of the business units/facilities, departments, etc. that detail the appropriate process/procedures that support proper documentation, billing and charging and they cannot all be listed here. Each employee is responsible for understanding the requirements of his/her job and how it is impacted by policy and regulation. See your respective supervisor or department head for direction regarding the availability of the appropriate policies.

Select corporate compliance policies that directly impact billing and charging include:

- Identity Theft Prevention (SP-1.28). This policy addresses the proper verification of the patient's identity at registration and the supporting program to follow when we believe a false identity has been presented or identity theft has occurred. Proper identification of the patient at time of admission is critical, as it could adversely impact that patient's care (or that of the identity theft victim due to incorrect information placed in their chart) as well as the reimbursement for services.
- Authentication Standards (SP-1.20). This policy defines the requirement for valid physician signatures on orders (including legibility, electronic signatures, use of signature logs, etc.) and the information needed in a valid verbal order. If an order is not properly authenticated per CMS standards, they will treat the order as if it doesn't exist.
- Sanction Screening (SP-1.18). Just as CMS requires properly authenticated/valid orders for all services provided, they also insist that healthcare entities ensure those orders are coming from providers that have not been sanctioned by the government. Accepting orders from sanctioned individuals not only invalidates the order (and therefore eliminates reimbursement for the service), but could lead to sanctions of the organization that accepts these orders and/or does not effectively screen its referral sources. The regulations also require healthcare organizations to screen all its employees and key vendors and bans them from doing business with sanctioned individuals in any way that may result in direct or indirect reimbursement from government programs (including anything that rolls up into a cost report); this includes administrative functions (i.e. a sanctioned physician cannot be employed in a purely administrative role as that cost would be included in the cost report).
- Coding. There are several policies that outline requirements for proper coding and the supporting processes, including:
  - Inpatient Coding policy SP – 1.21
  - Hospital-based Outpatient Coding policy SP – 1.22
  - Query Documentation for Hospital Services policy SP – 1.23
- False Claims Education (SP-1.26). The False Claims Act (FCA) is the government's primary weapon in enforcing accurate billing and documentation. If we routinely submit claims to government payors that are not supported by the medical record, for services that are not medically necessary, did not meet minimum quality standards, or other errors/deficiencies, then those bills could be considered false claims and subject to severe penalties under the FCA. The government routinely audits for these violations and aggressively enforces the standards.

ProMedica also has various auditing and monitoring practices to detect and correct errors (see Auditing & Monitoring section below) and a hotline to allow employees/others to report suspected violations so that they can be addressed (see Reporting section below).

### Examples:

Physician orders:

If a nurse practitioner writes an inpatient admission order stating 'admit to 4th floor' that would be considered an invalid order and the entire patient stay could be denied. First of all, admission orders must be given by a physician. Currently regulations do not allow a Mid-Level Provider (MLP) to write admission orders on their own authority. Further an inpatient admission status order must contain the words 'admit as an inpatient' or something very similar to be considered valid. Stating 'admit to a floor', 'admit to a Dr. X', or simply 'admit' does NOT meet CMS criteria for an inpatient admission. These orders need to be written as promptly as possible (inpatient status doesn't start until a valid order is entered) and must be written prior to the patient's discharge (patient status cannot be changed from O/P to I/P post-discharge).

Medical Record Documentation:

The use of EHR's enhances our ability to chart by exception and in some cases duplicate entries (i.e. copy & paste). This can be especially risky in O/P locations where consistent or similar patient issues are routinely treated. If the only documentation in a patient's chart is checked boxes with no descriptive narrative and/or that narrative is consistent across patients and copied from one chart to another, the end result can be multiple patient charts that look the same. CMS considers this 'cloning' of M/R. If M/R's are clones, government audit agencies will likely challenge if individualized patient care is being provided/documented and therefore if it's reimbursable. There is nothing wrong with the efficiency afforded via charting by exception. However, when looking at the patient's encounter as a whole, ensure the chart reflects the history/concerns/ complaints/treatment unique to that patient – copy and paste should be avoided without citation of the original author. Also, ensure all services provided are fully documented in the chart. When the chart gets to Medical Records, they can only code from the documentation provided. If documentations standards are not met, we will be unable to code & bill for those services.

Charge Entry/Coding:

Where practical, coding of patient claims should be performed by a certified coder. In those environments where codes are selected via an encounter form (or electronic equivalent) the services coded (i.e. established patient, level 3) should be selected by the provider. When charges are entered in the system (in any environment), the person doing so should be knowledgeable of the services provided and the provider/department should ensure documentation supports the charge entered. Do not guess when it comes to charge entry or coding. This will get more complex with the implementation of ICD-10. If needed, seek advice from facility M/R coders or the Compliance Dept.

## Fraud

Anti-fraud programs focus on correct billing and charging as noted above in regards to the False Claims Act as well as 'generic' types of financial fraud. Fraud is defined as an intentional misrepresentation of a material fact designed to influence another to act (or fail to act) to his or her detriment. In the healthcare environment that commonly occurs by submitting claims that are not supported by a patient's medical record (false claim):

- *an intentional misrepresentation* – the items/services listed on the claim were not provided
- *of a material fact* – materiality isn't based on the individual dollar items, but on the percentage of the claim and/or a pattern of misstatements
- *designed to influence another to act* – by submitting a claim a provider is requesting payment
- *to his or her detriment* – the payor is harmed if they pay claims in good faith that do not represent goods/services provided

Other types of fraud in healthcare are those perpetrated by patients/members, such as identify theft (patients using another's insurance card to pay for services – see the identity theft policy to address this issue) or member fraud (in which health plan subscribers claim dependents for coverage that are not eligible – see Paramount policies). Other types of fraud involve criminal acts not unique to healthcare, such as embezzlement and other financial irregularities that could involve employees, patients, vendors, or other third parties. The Fraud Policy (SP – 1.12) defines fraud and establishes investigative authority and procedures when such activity is suspected. Anyone may report suspected fraud by calling the Compliance Hotline or the VP, Audit & Compliance at 419-291-0230.

## Contracting

Contracting policies have been established to enable review of contracts to promote compliance with laws and regulations, e.g., Fraud and Abuse, Stark, antitrust, regulations for tax-exempt organizations, private inurement/intermediate sanctions, and IRS rules distinguishing independent contractors from employees.

### Standards:

- All financial arrangements (whether with physicians or non-physicians) must be in a current written contract that fully describes the terms of the agreement.
- All contracts shall be reviewed by legal counsel prior to execution.
- Agreements must be consistent with fair market value.
- There must be a legitimate business need for the services.
- Payments to physicians are contingent on a signed agreement and compliance with terms of agreement (i.e. submission of time sheets).
- Physician arrangements must not influence or induce referrals.

### Policies:

For specific requirements in contracting with physicians see the Physician Contract policy and with all others see the Contracts and Financial Arrangements with Non-Physicians policy, this includes leases, service contracts, purchases of real property, etc.

Note that in certain circumstances (generally a vendor to whom we provide protected health information (PHI) in order for them to perform a service on our behalf – other than patient care), these arrangements may also require a Business Associate Agreement (BAA). To determine if a BAA is required see the Business Associate Policy and attachments, which include a BAA questionnaire to walk you through the process of determining when a BAA or Confidentiality Agreement (CA) is needed. A BAA & CA are also attached and any proposed changes must be reviewed be Legal.

### Examples:

An example of when a BAA is required would be a collection agency to which we are giving patient billing information and asking them to pursue delinquent collections on our behalf.

An example of an appropriate confidentiality agreement would be a cleaning service for which we do not provide any PHI (not required for their service); however, they may be exposed to it while in the facility performing their duties. This is called an incidental disclosure under HIPAA and we would request the cleaning service to sign a confidentiality agreement to protect any such exposure.

## Patient Referrals

**Patient choice**

A basic premise of patient rights is the patient's right to make decisions regarding his or her care. This includes choosing the providers that provide that care. Often during the discharge planning process, or at other points in the healthcare continuum, the determination is made that the patient will need additional healthcare services. It is imperative to ensure that the patient and his or her designated decision makers are an active part of the planning and decision making process. In some cases, for example referrals to Nursing Homes and Home Care, we are required by regulation to provide the patient with a list of all of the providers of these services in the area. The *CMS Conditions of Participation for Hospitals* provide additional guidance regarding patient rights and patient involvement and choice in the discharge planning process.

**Inducements – Physicians & Patients**

Offering valuable gifts to beneficiaries to influence their choice of a Medicare or Medicaid provider is a violation of the Social Security Act. A person who offers or transfers to a Medicare or Medicaid beneficiary, any remuneration that the person knows or should know is likely to influence the beneficiary's selection of a particular provider, practitioner, or supplier of Medicare or Medicaid payable items or services, may be liable for civil money penalties (CMPs) of up to $10,000 for each wrongful act. The statute defines "remuneration" to include, without limitation, waivers of copayments and deductible amounts (or any part thereof) and transfers of items or services for free or for other than fair market value.

The definition of "remuneration" contains five specific exceptions:

- Non-routine, unadvertised waivers of copayments or deductible amounts based on individualized determinations of financial need or exhaustion of reasonable collection efforts.
- Properly disclosed differentials in a health insurance plan's copayments or deductibles.

- Incentives to promote the delivery of preventive care.
- Some services, such as companionship provided by volunteers, have psychological, rather than monetary value.
- Any practice permitted under the anti-kickback statute safe harbor

## Quality of Care

Substandard quality of care has been used as the basis of some False Claims Act and criminal liability actions. They have pursued these charges based on the premise that when providers submit a claim to the federal government (Medicare or other federally funded programs) the provider certifies that the services performed met care standards. Therefore if they can prove that quality of care issues were present, they may deem it to not meet the minimum quality standards or that it was so deficient that it constitutes a "worthless service" and determine a false claim was submitted.

As Healthcare payment structures are transforming, there is considerably focus on quality of care from the standpoint that quality and efficiency go hand in hand. The ProMedica Quality and Performance Improvement Department (PQPI) takes the lead on ensuring high quality patient care is provided throughout the system using an evidence based, data driven approach. PQPI monitors the reporting of quality indicators as required to CMS and other payers, and uses this data for systematic performance improvement activities.

## Use of Electronic Media

We must always be aware of protecting confidential information over which we have access or control, whether that is patient/member confidential information covered by the HIPAA regulations or other business information that is not for public consumption. In an electronic environment, that requires understanding basic controls over access, transmission, and posting of data.

### Standards:

- Emails containing confidential information should limit that information to what is minimally necessary to be communicated to the recipient.
- Emails with confidential content sent to an email address outside the ProMedica network (an address other than xxx@promedica.org) must be encrypted.
- If ProMedica emails are synced to portable devices, adequate security must be maintained on that device.
- Confidential information should not be posted to social media.

### Policies:

There are numerous HIPAA policies dealing with patient privacy (see next section). The Minimum Necessary Uses & Disclosures policy provides guidelines for disclosing only that information that is needed to carry out one's job responsibilities. The Email Usage & Message Management Policy clearly defines the proper use of email, including when encryption is required and employee's responsibility for protecting his/her user access. The Portable Devices policy establishes the requirements for accessing ProMedica information via a portable device and the employee's responsibility to then protect that data, including use of onboard security features and notification

to IT to wipe the device if lost or stolen. The Social Media policy explains what employees can/cannot disclose via social media as it relates to ProMedica activity.

### Examples:

To send an encrypted email:

- Type addressee and email body as you normally would.
- In the subject line, as the first item, enter [SECURE].
  - Make sure you include both brackets '[' and ']' and the word secure.
- This will encrypt the outgoing message and notify the recipient that they have a secure message and how to open it.

## Patient/Member Privacy Rights

Patient's expectation of privacy is ensured through the Health Insurance Portability and Accountability Act (HIPAA) and other regulations. These rules are extensive and ProMedica has provided a considerable amount of training on this subject in addition to multiple policies to communicate how the rules are to be implemented. The HIPAA policies are available on myProMedica along with an index for ease of reference and the Compliance & Privacy webpage has various articles and other reference material that is routinely updated.

To ensure compliance with HIPAA, one must first understand the definition of Protected Health Information (PHI) which is the foundation upon which the rules are based. PHI is information that is created or received by ProMedica; and related to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual. PHI also either identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual. PHI pertains to both living and deceased individuals. There are defined rules for 'de-identifying' data so that it does not contain PHI (see the Limited Data Set policy), but as a general rule if one person can determine the identity of the member/patient or to whom the information applies a HIPAA violation has likely occurred. Therefore, employees, physicians, volunteers, and vendors associated with ProMedica must be diligent in ensuring all communication regarding patients/members is appropriate. See the Workforce General Obligations policy for guidelines in this regard.

### Standards:

- All workforce members (including employees, physicians, volunteers) have a responsibility to protect PHI.
- Patient/member information can only be shared with those who have a legitimate need to know to perform their duties or as required under law.
- Workforce members are responsible for maintaining current knowledge of the HIPAA requirements/ ProMedica Policy and employing them in their daily activities. Management will facilitate this by providing training/education in various forms throughout the year.

### Examples:

Public knowledge of their privacy rights has resulted in numerous complaints to covered entities and government authorities, both of which must take these cases seriously. As a result, various examples of HIPAA enforcement are frequently in the news. Some examples from the headlines include:

Social Media:
Five California nurses were fired after allegedly discussing patients on Facebook. The nurses lost their jobs after an internal investigation and three weeks of administrative leave. While no details of the incident have been revealed, the CEO of Tri-City Medical Center has said that no patient names, photos or identifying information were included in the posts.

Unauthorized Access:
A Cardiothoracic Surgeon working at UCLA as a researcher sentenced in April 2010 to 4 months in prison for looking up patient medical records he was not authorized to view, i.e. his supervisor's, former coworker's, celebrities', etc.

In another example, 16 employees were fired at a Houston hospital for accessing the M/R of a resident who was hospitalized after being shot in an attempted robbery.

## Employee Responsibilities Regarding Detected Compliance Concerns

Employees must have a sufficient level of understanding of the Compliance Plan and related policies to comply with the requirements therein during the performance of their duties and be able to identify potential compliance issues as they arise.

### Policies:

In addition to understanding the rules, employees have an affirmative duty to report suspected violations through proper channels. As defined in the Problem Reporting and Non-Retaliation policy as well as the How to Report a Compliance Concern flowchart below, reports of suspected wrongdoing may be made through an employee's chain of command, calling the Compliance Dept. or calling the hotline. If the Compliance Dept. (or others) is investigating a report of non-compliance, all involved employees/workforce members are expected to fully cooperate with the investigation.

Employees also need to be aware of the following policies which may impact them:

- The Compliance Resource Tracking policy (SP-1.08) outlines the process we use to identify resources committed to compliance across the organization. This is facilitated by Finance and Dept. Directors are asked to identify costs expended in furtherance of our compliance initiatives, such as training, reference material, consultants, internal monitoring, etc.
- The Search Warrants policy (SP–1.15) provides guidance on what to do if presented with a search warrant by a government official. The first step is to view the ID of the presenting individual, get a copy of the warrant and contact the Legal Dept. See the policy for further details.

- The Unauthorized Visits by Government Investigators or Auditors (SP–1.16) specifies one's rights and responsibilities if a government official requests information/asks questions, whether they show up at work or at an employee's home. Issues covered include a right to legal counsel and/or a witness, the right to decline/postpone an interview, etc. If an employee agrees to answer questions, always be truthful and never guess/assume an answer. If unsure, obtain contact information, confirm your response and follow up with the investigator.
- Failure to comply with the ProMedica Compliance Plan may subject an employee to discipline as outlined below.

## Antitrust Compliance

The antitrust laws prohibit certain anti-competitive agreements and conduct. The federal government is responsible for enforcing the federal antitrust laws, and state attorneys general are responsible for enforcing the state antitrust law in their respective state. Federal and state governments investigate and pursue organizations suspected of being in violation. Violation of these statues can result in significant losses through financial penalties and criminal sanctions.

### Standards:

- Employees should be extremely cautious in discussions with competitors.
- Topics that are **not** to be discussed with competitors include:
  - Prices or other terms of sale
  - *Non-public* cost, volume, or sales data
  - Contract bids
  - Dividing customers or contracts
  - Dividing territories or product lines
  - Boycotting customers, competitors, or suppliers of services or goods.
- Any questions regarding planned discussion topics with competitors or suspicion of existing violations should be immediately discussed with the Legal Department.

### Policies:

The Antirust Compliance Policy is maintained by the Legal Department and is available on myProMedica. Questions may be directed to the Legal Department by calling 419-469-3622.

### Examples:

Some common examples of Antitrust Law violations include:

Price Fixing:

This occurs when two or more competitors agree on the prices they will charge for their services, unless that agreement is part of a legitimate joint venture (i.e., common ownership and control, joint ownership) or collaboration (i.e., substantial financial risk sharing, program of clinical integration, accountable care organization). In the healthcare environment, this could take the form of two competing hospitals discussing rate setting for outpatient services for purposes of negotiation with commercial insurance companies. This is different than one party consulting

*publically acquired* competitive pricing information (i.e. information obtained via the internet or industry publications) to benchmark its own data to remain competitive.

Price fixing can also occur when two or more competitors agree on the wages or compensation they will pay their employees. For this reason, competitors should not exchange their wage and compensation information. Competitors may consult with wage studies that meet the requirements of the antitrust information sharing safety zone, unless otherwise approved in advance by the Legal Department.

Allocating Services or Territories:
This is an agreement among competitors – actual or potential – not to compete for certain services or in designated geographic areas. For example, a services allocation would occur if two hospitals agreed that only one of them would provide cancer care and the other would cardiovascular care, such that they did not have to compete with each other in either service line. Also for example, a geographic allocation would occur if two hospitals agreed that one would operate outpatient rehab sites only on the west side of town, and the other would operate outpatient rehab sites only on the east side of town, such that the two hospitals did not have to compete with each other in the same area.

Group Boycotts:
This can arise when two or more competitors agree to refuse to do business with a third party. Competing hospital should not agree with each other that they will not contract with a particular payor or employer group. Certain competitor boycotts of other competitors can also be found to be unlawful.

See the Antitrust Compliance Policy for a more detailed explanation of these issues.

## Compliance for Vendors

The vendors with whom we do business are also expected to comply with basic regulatory, legal, and ethical standards. These are defined in the Corporate Compliance for Vendors policy (SP-1.27) and include issues such as Standards of Conduct, confidentiality, intermediate sanctions, improper influence, false claims, fraud, whistleblower protections/use of our hotline, etc. Vendors should also be aware of the False Claims Education Policy (SP-1.26), which provides guidance on the federal and state False Claims Act. These policies are made available to vendors registering with the Vendormate system and on ProMedica's public website.

# Auditing & Monitoring

## Objective:

To detect areas of potential non-compliance and provide for the development of corrective actions. Once corrective action plans are developed, appropriate personnel need to be updated regarding their status to avoid recurrence of the same issue.

What is the difference between Auditing and Monitoring?

- Auditing
  - A methodical examination and review performed by someone independent of the transaction/event.
  - ProMedica has an Internal Audit function that performs audits across the organization based on a risk assessment process.
  - Other audits can be performed by contracted entities, regulatory bodies, etc.
- Monitoring
  - Internal observation and assessment performed by parties with a role in the transaction/event.
  - ProMedica has a process for facilitating self-monitoring for various revenue producing areas, as well as coding and billing (see the Compliance Monitoring Log process below).
  - All areas are responsible for determining the appropriate amount of monitoring for their functional responsibilities, this may take the form of quality measures, charge verifications, etc.

## Policies:

Corporate policies have been established that address the following purposes under this element:

- Establish responsibilities for Auditing & Monitoring – see Auditing & Monitoring policy SP – 1.01
- Enterprise Risk Assessment process to evaluate internal and external risks facing the organization, identify remediation efforts, and determine if further auditing or monitoring is needed – see policy SP – 1.29.
- Risk assessment process to determine internal audit priorities and the following year's audit schedule – see Audit Scheduling/Risk Analysis policy SP – 1.02.
- Establish a follow-up and communication process to ensure any action plans developed in response to audit activity is implemented – see Response, Follow-up, and Resolution policy SP – 1.14.
- Outline the Compliance Monitoring Log process, which facilitates revenue-producing department's, coding's, and billing's self-monitoring. Reports summarizing this process are generated and supplied to senior leadership by the Compliance Department – see Compliance Monitoring Policy – SP – 1.07.
- There are several policies that outline requirements for proper coding, the supporting processes around coding, and auditing & monitoring of the coding process, including:
  - Inpatient Coding policy SP – 1.21
  - Hospital-based Outpatient Coding policy SP – 1.22
  - Query Documentation for Hospital Services policy SP – 1.23
  - Coding Compliance Education policy SP – 1.24
  - Coding Monitoring & Education policy SP – 1.25

- There are also several policies describing our administrative process around CMS' Recovery Audit Contractor (RAC) program, including:
  - Automated Process policy SP – 1.30
  - Complex Audit policy SP – 1.31
  - Immediate Offset/Refund process SP – 1.32

# Training

## Objective:

The purpose of conducting a training and education program is to ensure that each employee, contractor and any individual that functions on behalf of ProMedica is fully capable of executing his or her role in compliance with rules, regulations and other standards.

## Policies:

The Compliance Education & Training policy SP – 1.10 outlines the primary educational initiatives inherent in the ProMedica compliance plan and everyone's responsibilities thereto.

## Examples:

Some of the primary educational initiatives include:

- All new employees receive compliance training as part new employee orientation.
- All ProMedica employees complete annual online compliance training.
- Quarterly leadership compliance training is developed by the Compliance Department with input from the Compliance Liaison Council. This is presented to leadership each quarter, which then provide the training to their staff (as appropriate).
- Periodic articles addressing timely compliance issues are published in the various ProMedica system level, business unit, and institute newsletters and publications.
- The Corporate Compliance PMU course is required for all new supervisors and managers and attendance is highly encouraged for general staff and anyone in a non-management leadership role.
- The Education Sub-Committee of the Compliance and Privacy Council assesses training needs for the system and works to develop content to address the needs identified.
- Department specific educational needs for compliance matters unique to given areas are the responsibility of management of that area. Assistance with educational information/guidance is available through the Compliance Department.

# Reporting

## Objective:

The Reporting process establishes a method for receiving concerns regarding potential non-compliance and provides for the appropriate investigation and follow-up of such reports. A hotline is also provided as a mechanism to protect the anonymity of complainant and help prevent retaliation of good-faith reporters.

## Policies:

Corporate policies have been established that address the following purposes under this element:

- The Problem Reporting and Non-Retaliation policy states that all employees have an affirmative duty to report suspected situations of non-compliance. It further ensures that there will be no retaliation tolerated for a good faith report. See policy SP – 1.13.
- The Compliance Hotline policy SP – 1.05 establishes the anonymous hotline available for employees, members, vendors, and patients to use in reporting suspected compliance issues.
- The Compliance Issue Resolution policy SP – 1.06 establishes the responsibility of the Compliance Department/Compliance Officer to either investigate reports of suspected non-compliance or refer issues received through the hotline to the appropriate personnel (if not an issue addressed by our Compliance Plan).

## Examples:

A variety of types of calls come through the compliance hotline. For instance, a caller may report a potential privacy breach. This would be investigated/addressed by the Privacy Officer. This may include reporting the breech to the Office of Civil Rights, notifying the patient, and employee discipline per policy.

In some cases, the calls are referred to others. For example, some callers have Human Resources concerns or may have questions for Paramount Members Services. Once it is determined that the issue is not compliance or privacy related, the correct contacts are notified to follow-up.

All significant calls are entered into a database and monitored to ensure follow-up and identify trends and patterns that may need to be addressed.

# Discipline

## Objective:

Provide for the consistent enforcement of appropriate disciplinary action when employees intentionally violate the compliance plan.

## Policies:

Any employee (regardless of position) may be subject to discipline, up to and including termination, if it is determined that his/her actions (or inactions) constituted a *willful violation* of law or a *willful failure* to adhere to ProMedica's compliance standards. Note that there is a difference between intentional/willful misconduct and mistakes. People make mistakes; the goal when errors are reported is to correct them (and if necessary disclose and refund overpayments received). If we allow an error of which we are aware to continue, this could be interpreted as *intent* to commit fraud and we may be subject to legal action, large fines, and penalties (see Remediation section). See your business unit's Human Resource policies for further information regarding discipline.

## Examples:

Disciplinary action, including suspension or termination, may be taken against any person who:

- Authorizes, or participates, directly or indirectly, in any action that constitutes a violation of applicable laws or Hospital policies.
- Fails to promptly report a compliance incident or withhold information concerning a violation of which s/he becomes aware.
- Supervises a person involved in a compliance violation to the extent that the circumstances reflect inadequate supervision or lack of appropriate diligence by supervisor.
- Attempts to retaliate or participates in retaliation, directly or indirectly, against a person who in good faith reports a compliance incident or encourages others to do so.
- Make a report of a compliance incident which is known (or should be reasonably known) by the reporting person to be false or misleading.
- Fails to cooperate fully with the hospital's efforts to investigate or otherwise address a Compliance Issue.

# Remediation

## Objective:

Establish a process for disclosing identified violations and making appropriate reparation in a timely manner.

## Policies:

If we identify an error that resulted in receipt of overpayments from governmental programs (i.e. Medicare, Medicaid, etc.) we will quantify the overpayment, self-disclose the error to the proper agency/authority, and reimburse the overpayment to the proper payor (i.e. the MAC, Medicaid, etc.). The Voluntary Disclosures to Third Parties policy SP – 1.17 establishes the procedures, responsibilities, and timeframes for properly notifying outside agencies of violations that must be reported.

## Examples:

Issues that we will disclose to third parties include:

- Overpayments received due to billing/coding/documentation errors are typically refunded to the MAC, Medicaid, etc. for issues such as:
  - Services incorrectly coded and/or billed
  - Lack of Medical Necessity for services billed, but not supported by medical record documentation
  - Missing required elements of a billable service that are not supported by the medical record
- Violations of other rules covered under our Compliance plan would be reported to the appropriate authorities.

## Other Compliance Plans

This document (along with the referenced links) defines the full scope of the ProMedica Corporate Compliance Plan. However there are several subsidiary plans that integrate with the corporate Plan for those areas with specific or unique regulations. These areas are below with links to their respective documents:

- Insurance
- Laboratory
- Rehabilitation
- Senior Services / Long-term Care
- Home Care & Hospice – in development
- Transportation – in development

## Questions & Answers

**Q:** How does this apply to me?

**A:** Everyone is responsible for being alert to potential problems and reporting all known or reasonably suspected problems through the proper channels. The nature of potential concerns will vary based on the area in which you work. Fraud and other terms of noncompliance take many forms and can occur anywhere; therefore, everyone needs to be alert for the signs.

The fraud and abuse statutes around patient billing are not simply a Financial Services issue; indeed by the time the information gets to billing, it sometimes may be too late to get the necessary documentation to make the claim acceptable to Medicare or Medicaid. The billing process starts at admission by getting the right diagnosis code on the system. At the point of care, appropriate levels of documentation need to be recorded in the chart to support the coding assigned by medical records. Ensuring accurate billing is a team effort that requires attention at many levels of the organization.

**Q:** When do I call the hotline?

**A:** Any concerns should first be reported to management of the area where the issue was noted. The manager then needs to contact the Director of Compliance and/or the Vice President of Audit & Compliance to determine appropriate action.

If for some reason an employee/patient/resident/member/vendor/etc. is not comfortable with normal reporting channels, s/he should either call the Director of Compliance and/or the Vice President of Audit & Compliance directly or contact the Compliance Hotline.

Regardless of how you report, you will be protected from retaliation for any good faith report of perceived noncompliance that you make.

**Q:** Who answers the hotline?

**A:** The hotline will be answered by voice-mail asking the caller to leave all relevant information. It is monitored by the Compliance Department.

**Q:** Do I have to give my name if I call the hotline?

**A:** NO. There will be no attempt to identify callers to the hotline. However, if the caller wishes to leave his/her name it would make investigation easier by allowing the Director of Compliance and/or the Vice President of Audit & Compliance to contact the reporting individual and obtain more information or clarification as needed.

**Q:** What information do I need to provide if I call the hotline?

**A:** The more information you can provide, the easier the investigation and the greater the probability of action being taken. Please provide not only what happened, but where, how, when (or for how

long), and by whom (if appropriate). Also, do not forget to say where the evidence can be located. If you don't have the answers to all these questions, provide as much information as you can.

**Q:** What happens after a hotline call is received?

**A:** That will vary with the type of call received. Generally, the Director of Compliance and/or the Vice President of Audit & Compliance (or their designee) will try to substantiate the claims "behind the scenes" based on available evidence before involving anyone else. If it is a billing related issue, management of the department(s) involved will be contacted to review the issues and develop action plans as appropriate. If it is a report of an individual's fraud (i.e. misappropriation of assets), appropriate action will be taken.

**Q:** If I detect a recurring billing error, but it is only a very small amount of money, do I need to report it?

**A:** YES.

**Q:** Will every call result in an audit?

**A:** No. An audit is only required if there is a question as to whether a problem exists. If the problem is known and a solution can be identified through working with management of the departments involved in the process, an audit is not necessary. However, the Audit Department may be involved (as needed) in assisting management in the quantification of past exposure to the organization.

**Q:** What if I suspect a problem, but am not sure of the regulations and/or don't know the extent of the risk?

**A:** Contact the Director of Compliance and/or the Vice President of Audit & Compliance. S/he can either clarify the applicable regulations or help find the answers. If a question still exists as to whether there is a violation, an audit may be appropriate and the details of that process can then be discussed.

**Q:** Who is responsible for identifying compliance problems and solutions?

**A:** **Everyone**.

**Q:** If I catch someone stealing from ProMedica, is that fraud that should be reported to the hotline?

**A:** Theft against ProMedica should always be reported immediately to the Security department or your supervisor.

**Q:** If a problem is discovered in my area, whom should I tell other than the Director of Compliance and/or the Vice President of Audit & Compliance?

**A:** Unless there is a reason you are uncomfortable doing so, you should tell your immediate supervisor. The Director of Compliance and/or the Vice President of Audit & Compliance will ensure that appropriate levels of management are notified depending on the issue being reported.

# How to Report a Compliance Concern