Table of Contents

Organizational Orientation:

Compliance and Ethics Information:

Introduction to Presbyterian

Purpose

This is an abbreviated version of organizational orientation and required compliance information. It is designed for workforce who will be onsite for a short period and/or will not have access to more formal orientation or computer-based training modules.

(**NOTE**: The term "workforce" includes employees, students, volunteers, contractors, vendors, and any other individuals performing work or training activities at a Presbyterian facility or as part of Presbyterian operations.)

Welcome to Presbyterian!

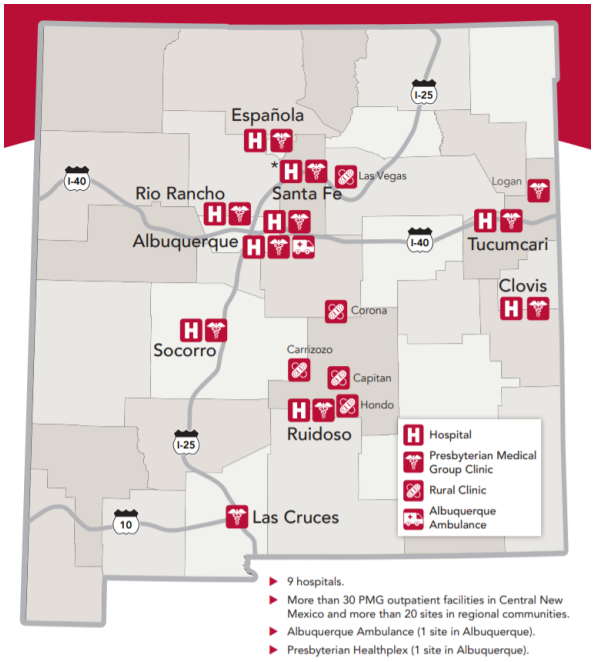
Presbyterian Healthcare Services (PHS) is a locally owned and operated healthcare system known nationally for our extensive experience in integrating healthcare financing and delivery. Read more about Presbyterian.

PHS is comprised of two business units:

- Presbyterian Delivery System (PDS), and
- Presbyterian Health Plan (PHP).

Presbyterian Delivery System (PDS)

The Presbyterian Delivery System is a not-for-profit healthcare system that has grown from a small tuberculosis sanatorium founded in 1908, to a system of nine hospitals, a multi-specialty medical group with more than 900 physicians and advanced practice clinicians.



Presbyterian Health Plan (PHP and PIC)

Presbyterian Health Plan (PHP) is a statewide health maintenance organization; Presbyterian Insurance Company (PIC) provides more traditional health insurance products. Together, they insure more than 600,000 members throughout New Mexico. PHP products include Commercial (employer-sponsored and individual) and Government (Medicaid, Medicare and other) programs. PHP is also one of four health plans contracted with the New Mexico Human Services Department Turquoise Care program to serve Medicaid members. PHP/PIC is a for-profit entity.

Board Leadership

Community-based volunteer boards are the cornerstone of Presbyterian's governance system. The PHS Board, with key supporting committees in Compliance and Audit, Executive Compensation, Finance, Governance, and Quality, is ultimately responsible for the entire system. The overall governance structure also includes a volunteer board or governing committee for each community, the Medical Group, the Foundation, and PHP. The community affiliate boards report to the PHS Board, govern in the communities where they reside, and are charged with assessing and ensuring the appropriateness of the health care services provided.

Workforce

Presbyterian's workforce consists of more than 13,000 employees, plus contracted staff, students and volunteers. As part of its workforce, PHS employs over 900 physicians and advanced care practitioners who provide both primary care and specialty services.

Medical Staff

Contracted and hospital privileged physicians play a role in the leadership and delivery of health care. Presbyterian's delivery system has more than 2,000 credentialed providers, representing over two dozen recognized specialty fields. Over 17,000 practitioners across the state contract with PHP and over 90% of these are independent physicians who practice medicine in PHS facilities and other facilities throughout New Mexico.

Contractors and Suppliers

PHS contracts with temporary nurses, locum tenens providers, and other clinical and non-clinical workforce. As part of initial orientation, these contracted workforce members receive information on compliance, safety, hazardous chemicals, disaster preparedness, hand washing/infection prevention, security, and other job-specific information.

BACK TO TOP

The Presbyterian Egg: Purpose, Vision, Culture, and Strategy

The Egg

Presbyterian exists to improve the health of the patients, members and communities we serve. Presbyterian has summarized its purpose, vision, culture and strategy in a format we call the "Egg." See below for a picture of the Egg. Read more about the Presbyterian Egg

YOU are Part of the Mission

By joining Presbyterian as an employee, volunteer, student, contractor, vendor, consultant, board member, or other interested party, you are helping us to ensure all of the patients, members and communities we serve can achieve their best health.
Thank you!

BACK TO TOP

Code of Conduct

December 2024 revision

In addition to the Presbyterian Egg, our Code of Conduct describes the behavior expected of our workforce in providing services to our patients and members. Leaders, employees, independent providers, contractors, volunteers, students, vendors and board members are accountable for these core responsibilities.

Read Code of Conduct (English) or **Spanish**

BACK TO TOP

False Claims Act Education

Specific Information Regarding False Claims Liability, Whistleblower Protections and Related PHS Policies

Presbyterian Position

PHS will not submit or cause to be submitted false or fraudulent claims. Furthermore, employees, contractors and subcontractors of PHS can be terminated for filing or causing to be filed false or fraudulent claims. PHS strictly prohibits the submission or participation in the submission of any false claims.

Laws

The Federal False Claims Act (FCA) provides liability for individuals who file or cause to be filed false or fraudulent claims. Examples of false or fraudulent claims include, but are not limited to:

- billing for services not rendered;
- billing for undocumented services;
- double-billing for items or services;
- making false statements in connection with the provision of services;
- participating in kickback schemes;
- including improper entries on cost reports;
- billing for medically unnecessary services; and
- assigning incorrect codes to secure higher reimbursement.

The government may impose fines or bring a lawsuit to recover fraudulently-obtained monies. In addition, individuals, known as whistleblowers, may bring such a lawsuit on behalf of the government and, if successful, may share in a portion of the recovery.

The New Mexico Medicaid False Claims Act is very similar to the FCA. Like the FCA, it allows individuals, known as whistleblowers, with knowledge of fraudulent activities to bring a lawsuit on behalf of the government to recover fraudulently-obtained monies and to share in the recovery, if successful.

The Program Fraud Civil Remedies Act (PFCRA) gives federal agencies the ability to initiate administrative proceedings on claims of $150,000 or less, when the U.S. Department of Justice elects not to pursue False Claims Act remedies for claims.

Whistleblower Protection

The FCA and the New Mexico Medicaid False Claims Act also provide statutory protections for whistleblowers. Under these laws, an employer is prohibited from retaliating against an employee who reports fraudulent activities.

Duty to Report

PHS requires that any workforce member having knowledge of or suspecting the existence of fraudulent activities immediately contact a direct supervisor, the facility's Human Resource Business Partner, or another member of the facility management staff. Workforce members may also report fraudulent activities to:

- Andrea Kinsley, Vice President Corporate Compliance, via telephone (505-923-8547) or email (akinsley@phs.org);
- Compliance Hotline (1-888-435-4361). Reports made to the Compliance Hotline may be made anonymously 24 hours a day, 365 days a year.

Related Policies

PHS has implemented policies aimed at preventing the filing of false claims. Those policies include False Claims Act Education (COM.PHS-E.105), Required Training (HR.PHS-E.335), and Compliance and Ethics Program (COM.PHS-E.103). In addition, PHS will require that all members of the PHS workforce receive information on these issues.

BACK TO TOP

HIPAA: Information Privacy & Security

Patient or Member Authorization Required for Disclosure of Information

General Rule: In general, you may **not** disclose protected health information (PHI) about individual patients or members without that individual's permission. HIPAA requires a signed authorization form from a patient or member before that person's information may be accessed or disclosed.

Exceptions: There are situations when the requirement to obtain an authorization does ***not*** apply:

- if the information is being used for healthcare *treatment*, *payment* or *operations*
- if the patient or member is requesting information about him or herself
- if there is a legal requirement to report protected health information to a government agency
- other exceptions are described in the Presbyterian Notice of Privacy Practices

Reporting Inappropriate Disclosures of Confidential Information

If you become aware that patient or member information has been inappropriately or accidentally disclosed, **you must report that disclosure to the Presbyterian Compliance Hotline immediately:**

1-888-435-4361

- Presbyterian will conduct an investigation and risk assessment to determine whether the disclosure meets the definition of "breach" as provided in the HIPAA regulations.
- If the information disclosed was in an electronic format, please also contact the Presbyterian Information Technology Service Desk immediately at (505) 923-6825, so that rapid action can be taken to safeguard information.
- You will be asked for specific information about the disclosure so that Presbyterian can complete its investigation.

Accessing Patient or Member Information for Self, Friends, Family or Others

Workforce members may not use their Presbyterian access to protected health information to read, copy or modify patient or member information regarding themselves or anyone for whom they are not officially providing care or services.

If a member of the PHS Workforce desires access to his or her own patient or member information, a request must be made through standard channels:

- Contact Medical Records Department of the Presbyterian facility,
- Access via a "MyPres" account online, or
- Contact the workforce member's own health care provider.

Individual Workforce Are at Risk

Inappropriately accessing patient or member information is a violation of federal law and potential grounds for termination of the employment or contractual relationship with Presbyterian.

Under HIPAA Privacy regulations, both organizations and/or individual employees, contractors, students, volunteers and business associates are subject to criminal and monetary penalties for violating privacy standards. If you have questions about the privacy of Protected Health Information (PHI), you may contact the Presbyterian Privacy Officer at (505) 923-6176.

Patient and Member Rights Regarding Protected Health Information

Presbyterian affords patients and members certain rights in accordance with HIPAA Privacy Regulations; these rights are described in more detail in the Presbyterian Healthcare Services Joint Notice of Privacy Practices (also available from Admitting / Registration or Compliance) and in Presbyterian policies. Patient and member rights include the right to:

- See and get a copy of health information
- Amend incorrect or incomplete health information
- Request confidential communications of health information
- Request restrictions of health information
- Request an 'Accounting of Disclosures' of health information
- Receive a paper copy of the Notice of Privacy Practices

If you have any questions about how these rights apply to a given situation, please contact the Presbyterian Privacy Officer at (505) 923-6176.

Minimum Necessary Principle

Under the HIPAA Privacy regulations, most use and disclosure of patient information is limited to the "minimum necessary" needed in order to meet the intended purpose (for example for insurance payment or various other healthcare business operations). The regulations, however, allow for certain key exceptions to this principle, including the following situations where "minimum necessary" does not apply:

- For treatment of a patient when sharing information with other providers involved in that patient's care.
- When disclosing information to the patient or member, or that individual's legally authorized representative.
- When disclosing information in accordance with an individual authorization (in this case the authorization will state what type of information may be disclosed.)
- When disclosing information in accordance with federal, state and local law, or to the US Department of Health and Human Services for the purposes of HIPAA compliance monitoring.

Disclosure of an individual's entire medical record by Presbyterian requires special justification and documentation. Contact the medical records department for more information.

Confidential Information

You are required to safeguard all Presbyterian "Confidential information." Confidential information includes 'Protected Health Information' (PHI), but also includes company financial information, operating methods, marketing strategies, and lists of patients, customers, members or employees.

Workforce members may not use or disclose confidential information obtained in the course of performing work at Presbyterian for the purpose of advancing any private interest or otherwise for personal gain. Additionally, confidential information or access to such confidential information should only be used in the manner for which it is intended. Disclosing confidential information in an unauthorized way is prohibited.

Reasonable Safeguards to Protect Patient Information

Encryption: According to the Presbyterian policy on Encryption, all Presbyterian business associates and workforce members are required to encrypt any Confidential Information stored on a personal computer or electronic storage device (such as flash drives or external memory devices).

Other Safeguards:

Presbyterian protects patient information from inadvertent disclosure, loss or theft through a variety of other physical safeguards, administrative processes and technical security mechanisms. Workforce members should adhere to these safeguards when using or disclosing Presbyterian patient or member information, including:

- Always use at least two identifiers to correctly identify customers (i.e. match on *at least* full name and date of birth.)
- When searching for individual records in a computer system, always use additional identifiers (such as address or account number) to resolve any duplicate search results.
- Conduct verbal communications in a discreet manner, especially in public areas
- Do not leave paper records and files in public view, on fax machines or copiers; turn over papers, close files and put them away.
- Close electronic records containing patient information when not in use; log off computer applications when not actively using.
- Always check *each page* of any paperwork delivered or handed to a customer first to ensure that it is going to the correct individual.
- Never remove hard copy patient medical records from the facility;
- Mobile devices used to send or store Protected Health Information must be encrypted (NOTE: password protection is NOT encryption – contact your mobile device carrier to for encryption instructions.)
- Do not transmit patient information via text message; instead use encrypted email or secure websites.
- Exercise caution when accessing PHS patient information systems from outside PHS facilities, and do not leave PHI unattended on screen.
- Never post Presbyterian Confidential Information or Protected Health Information to social networking websites.

Protection of Passwords

Passwords issued to PHS workforce members, that allow workforce to access Presbyterian information systems, must be safeguarded.

Passwords should not be:

- Shared, posted or left in an easily accessible location
- Created in such a way that they are easily guessed
- Passwords should be unique and not reused for multiple applications and systems

Remember, each individual is responsible for any system activity conducted using his or her password.

Login Monitoring

If problems with login, assigned passwords or multi-factor authentication are encountered, this could be a sign of a stolen or inappropriately modified password. In such instances, workforce members should seek assistance from the Presbyterian Information Technology Service Desk at (505) 923-6825.

Malicious Software: Viruses, Worms, Trojans and other Invasive Software

Malicious software programs, such as computer viruses or worms, represent a threat to clinical and business information systems and as such to patient care and service. In order to protect Presbyterian information systems:

Business Associates and Workforce members should not:

- Insert any disc or portable drive or download any software onto a Presbyterian computer workstation without first obtaining permission from Presbyterian Information Security.
- Open email attachments or click on links from unrecognized senders when utilizing a Presbyterian computer workstation; instead these should be reported via the Report Phishing Protection button in Outlook or by forwarding to abuse@phs.org.
- Ignore virus alerts and warnings; instead these should be reported to the Presbyterian Information Technology Service Desk at (505) 923-6825.

HIPAA Policies and Resources

Presbyterian Healthcare Services (PHS) has a comprehensive set of HIPAA Policies designed to interpret the HIPAA Privacy and Security regulations for the PHS workforce. These policies are available to workforce members through the Presbyterian Electronic Library (PEL) on the Presbyterian Intranet (PresNet) or from the Presbyterian Compliance Department. If you have questions about any of these policies, you may call the Presbyterian Compliance Department at (505) 923-6176.

BACK TO TOP

Information Technology Acceptable Use

All Presbyterian Healthcare Services (PHS) information technology and services are provided for the purpose of promoting and executing PHS business activities, are the property of PHS and/or specifically designated business partners.

Security and Monitoring

Use of PHS information technology services is subject to monitoring, without consent or notice, in accordance with Presbyterian policy. PHS may monitor electronically transmitted messages and information. There is no guarantee of privacy for the individual user regarding electronically stored or transmitted content using PHS information technology services.

Individual users consent to such monitoring by their use of the services. Any user of PHS information technology services is advised that if monitoring reveals possible indications of unacceptable system use, the discovery will lead to remedial action, up to and including termination of an educational, business or medical staff relationship. In addition, if such monitoring reveals possible indication of criminal activity, information systems personnel may provide the information from such monitoring to law enforcement officials.

Use of PHS computer hardware and software is a privilege, which can be withdrawn by PHS without notice. If PHS management deems that a violation of the information technology policies and procedures has or might have occurred, then the privilege of using those systems may be withdrawn indefinitely, without notice.

Secure Email

Email sent to an address outside the Presbyterian network that contains Presbyterian Confidential Information *must be encrypted.* This applies to emails containing confidential information in either the body of the email or in an attachment, and applies even if the attachment is password protected. To encrypt email sent from a phs.org address, simply include the phrase, “SEND SECURE” in the subject line of that email. The email recipient will be directed to a secure website and asked to login in order to receive the email.

General Prohibitions

All users of the computer and internal or external communications systems are expected to use PHS information technology services in an appropriate manner. The following are examples of prohibited conduct and each may result in corrective action, up to and including termination of employment or contractual services.

a. Disclosure of Confidential Information (including, but not limited to financial information or PHI) to any unauthorized individuals or entities.
b. Use of another person’s password, PIN, logon ID or access code, or disclosure of one’s own passwords without IS or managerial approval.

c. Use of Social Media, including accessing personal social media websites from a Presbyterian computer or posting images of, or information about a Presbyterian patient or member.
d. Disclosing / Storing PHI on an unencrypted mobile device. Avoid use of mobile devices to store or send PHI; if your work requires such use, then device must be encrypted to avoid potential federal HIPAA sanctions.
e. Unauthorized endorsement: Communicating material information that could be perceived as an official company position or endorsement without proper management approval.
f. Harassment: The transmission or storage of any discriminatory, offensive, disruptive, harassing or unprofessional message or language; derogatory statements about a person, product or organization, or any defamatory information. Prohibited material includes, but is not limited to, profanity, sexual comments or images, racial slurs, gender-based comments, or comments that would offend another person because of their age, gender, sexual orientation, religious or political beliefs, national origin or disability.
g. Solicitation: Soliciting, except as provided for in the PHS Solicitation/ Distribution/Posting policy and as approved by management. Also includes the transmission or posting of any information or material that would violate the PHS Solicitation and Distribution policy (HR.PHS-E.400).
h. Leaving confidential information unattended: Failure at any time to clear from view, after use, sensitive or confidential information on PC or terminal screens that are unattended.
i. Modifying the configuration or setup of any PC without information services direction. A user may not install unauthorized software.
j. Participating or engaging in activities that violate PHS policies or standards.
k. Involvement in scams, schemes, unlawful and/or illegal activities.
l. Intentional disruption of information technology services.
m. Playing games via the network or internet.
n. Violation of copyright: Failure to obtain written permission from the author or artist prior to using copyright material, including unauthorized posting, transmission, or downloading of copyrighted material, trademarks, and service marks.
o. Unauthorized access. This includes, but is not limited to:
    1. Accessing patient or employee information without a legitimate business need and authorized access;
    2. Misrepresenting an individual's identity or the source of communications or data;
    3. Accessing or attempting to break into any confidential or private information without authorization including servers, email or voicemail accounts, PC files or mainframe applications;
    4. Import or export of any governmentally controlled information to or from unauthorized locations or persons, without appropriate licenses or permits;
    5. Modifications of files without owner's permission;
    6. Cracking of passwords. (The existence of a file and access thereto does not grant permission or authorization to read it.)

This is not an exhaustive list and is intended only to exemplify the kinds of abuses that are prohibited by Presbyterian policy.

BACK TO TOP

Reporting of Patient Abuse, Neglect and Misappropriation of Property

Zero Tolerance for Abuse

Presbyterian has a zero tolerance policy for any type of abusive behavior by members of the Presbyterian workforce toward patients. The following behaviors are grounds for immediate suspension and/or termination of employment or other business relationship:

- Abuse of Patients
- Improper Treatment of Patients
- Harassment (including sexual harassment) of patients, employees or customers
- Theft or Attempted Theft of Property Belonging to Patients, Visitors, Employees or Presbyterian

What Must Be Reported?

The following types of abuse must be reported to the appropriate authorities (appropriate authorities are listed in the "How to Report Abuse" section below):

- All suspected abuse, neglect or misappropriation of property of a patient, if the suspected abuser is part of the Presbyterian workforce
- All suspected abuse or neglect of a child, no matter who the abuser is.
- All suspected abuse, neglect or exploitation of a vulnerable adult, no matter who the abuser is.

What About Domestic Violence or Adult Sexual Assault?

There is no **legal mandate** to report the following types of abuse (unless this abuse is against a child or an elder / vulnerable adult):

- Domestic or dating violence
- Adult sexual abuse or assault

Clinicians are required to screen for and document signs of these types of abuse in the patients that they see. (See Abuse, Neglect and Misappropriation of Property Recognition, Identification, Reporting and Follow-up policy, PC.PDS.129)

In addition, referrals to support services are to be offered when a patient says that they have been abused, or show signs of having been abused.

Reporting of these types of suspected abuse, however, generally requires the written authorization of the person who is the suspected victim. **You should not report these types of abuse (domestic/date violence or adult sexual assault/abuse) without a written patient authorization or permission from the Legal Services Dept.**

Time Frame to Report is 24 HOURS

Suspected abuse, neglect, or misappropriation of property must be reported **immediately** (as soon as practical and not later than 24 hours from knowledge of the incident). The incident must be reported within 24 hours, even if the facility has begun its own investigation into the matter and has not yet completed that investigation.

Who Must Report?

You must report if you are:

- An employee of Presbyterian
- A contractor of Presbyterian
- A volunteer for Presbyterian
- A student at Presbyterian

NOTE: All the categories above include, but are not limited to:

- licensed physicians, residents or interns
- registered nurses, visiting nurses, or social workers acting in an official capacity;
- members of the clergy who have information that is not privileged as a matter of law.

Your Responsibilities

When an incident of abuse, neglect or misappropriation of patient property is suspected, the individual who suspects or becomes aware of incident must immediately:

1. Notify the medical social worker, house supervisor, clinical lead, practice administrator, on-call administrator or charge nurse,
2. Work with the supervisor, charge nurse or administrator to make sure that the first page of the Incident Report Form is filled out according to the Incident Report Form instructions. For additional assistance, contact the Presbyterian Risk Management Department (505-923-8801).

New Mexico state law is very specific that the individual who has a ***direct knowledge*** of an incident of or signs of abuse, neglect or exploitation ***must*** be the one to fill out the first page of the Incident Report Form.

If you are the one who becomes aware of abuse, neglect, or exploitation then you will be required to fill out the first page of the form. You will have help and assistance available to you to answer questions from the notified medical social worker, house supervisor, clinical lead, practice administrator or on-call administrator, but the law is specific that you must complete the first section of the form.

Report Will Be Made to Two Different Agencies

The medical social worker, house supervisor, clinical lead, practice administrator or on-call administrator must ensure that the Incident Report Form is filed with the New Mexico Department of Health Improvement **and** one of the following agencies:

- Child Protective Services or
- Adult Protective Services.

In Emergencies

In an emergency situation, the first things that you should do are:

- Make sure the patient or other threatened individual is safe
- Notify your facility's security department or area
- Discuss with Presbyterian supervisor/manager and/ or Risk Management Department (505-923-8801) immediately and following their direction
- Cooperate in reporting to appropriate law enforcement and regulatory agencies

Abuse By a Member of the Workforce

If a member of Presbyterian's workforce (an employee, contractor, volunteer, student or other workforce member) is suspected of patient abuse it is especially concerning. Steps outlined above for Emergency situations should be followed in these cases (make sure the patient is safe, notify Security, and tell your supervisor immediately.)

The same process for reporting the suspected abuse should be followed in these cases as in any others.

Protection From Retaliation Against Those Who Report

Anyone who reports actual or suspected abuse, neglect or exploitation in good faith may not be retaliated against; this is a requirement in both in New Mexico state law and in Presbyterian policy.

NOTE: Intentionally making a false report of abuse, neglect or exploitation is prohibited.

Related Presbyterian Policies

Some key policies that you can refer to for more specific information are:

- Abuse, Neglect and Misappropriation of Property - Recognition, Identification, Reporting and Follow-up policy (PC.PDS.129) – reporting process for Albuquerque and Regional Delivery System
- Workplace Violence policy (HR.PHS-E.322) – what to do in emergency situations
- Patient Complaint and Grievance Management policy (PC.PDS.171) – how to handle patient complaints in general and in particular complaints about misappropriation of property

NOTE: All of these policies are available on the Presbyterian Electronic Library (PEL). If you do not have access to the PEL, you may contact the PHS Compliance Department to obtain copies.

BACK TO TOP

Conflict of Interest Information

Non-Employee workforce are required to disclose any potential "Conflicts of Interest."

Examples of Types of Conflict of Interest: A conflict of interest can potentially occur in situations where an individual has close ties or loyalties to more than one group or organization. For members of Presbyterian's workforce, some examples of possible conflicts of interest include the following situations:

- **Employment or Compensation**: You, your company, or one of your company's subsidiaries may employ or compensate managers, executives, medical staff, board members or employees of PHS or PHP

- **Personal Relationship**: You or one of your family members are related to managers, executives, medical staff, board members or employees of Presbyterian Healthcare Services or Presbyterian Health Plan (PHS or PHP)

- **Company Relationships with PHS Leadership:** Your company's managers, executives or board members are related to managers, executives, medical staff, board members or employees of PHS or PHP

- **PHS Workforce Serving on Company Board**: A PHS or PHP manager, executive, medical staff member, board member or employee serves on the advisory boards or the board of directors of your company or any of its subsidiaries

If one of the situations listed above applies to you, it is possible that there is a conflict of interest that Presbyterian will need to consider in defining your work assignment:

- **It doesn't mean that you may not work for or train at Presbyterian**. Presbyterian will review each situation on a case by case basis, and make a decision based on the Presbyterian Conflict of Interest policy (HR.PHS-E.317).

- **It does mean that you must disclose a possible Conflict of Interest** situation to your Presbyterian contact, the Presbyterian Human Resources department and/or a Compliance Staff member before you start work or as soon as you are aware of the conflict.

- **Questions**: You may contact the Presbyterian Human Resources Department at (505) 923-8750 (**AskHR@phs.org**) or the Vice President for Corporate Compliance, Andrea Kinsley, at (505) 923-8547 (**akinsley@phs.org**) for assistance with any questions related to Conflict of Interest.

BACK TO TOP

**********End of Document**********