Code of Conduct

Judi Health™

Judi Rx, Inc. and all its divisions and subsidiaries, including Judi Health, LLC (hereinafter referred to as "Judi Health")

Table of Contents

A Message From Our Chief Executive Officer (CEO)

A Message From Our Chief Compliance Officer (CCO)

Helpful Resources

05 OUR CODE OF CONDUCT

- Purpose and Overview
- Our Guidelines for Good Decision Making
- Speaking Up and Reporting Concerns

12 OUR WORKPLACE

- Staying Safe and Healthy at Work
- Providing Equal Opportunities
- Preventing Harassment
- Using Our Physical and Electronic Assets
- Preserving Private Data
- Implementing Artificial Intelligence

20 OUR CUSTOMERS

- Vendor Management
- Working with the Government
- Interacting with Healthcare Professionals
- Giving Gifts Responsibly
- Avoiding Conflicts of Interest

25 OUR STANDARDS

- Keeping Accurate Records
- Protecting Confidential Information and Intellectual Property
- Fighting Fraud, Waste, and Abuse
- Communicating with the Public
- Proper Marketing Practices and Disclosures
- Following Anti-Corruption and Bribery Laws
- Understanding Money Laundering
- Avoiding Insider Trading
- Competing Fairly
- Cooperating with Government Investigations and Audits

37 OUR COMMUNITY

- Our Responsibility to the World
- Contributing Outside the Workplace
- Honoring Our Environment

"AT JUDI HEALTH, WE KNOW HEALTHCARE IS A JOURNEY."

A Message From Our Chief Executive Officer

At Judi Health, we know healthcare is a journey. Helping people navigate that journey and removing obstacles to their care is what we do best. We do our work with purpose and integrity, guided by our shared Values and our Code of Conduct ("Code").

To put it in the simplest possible terms, the Code helps you do what's right. It illustrates what matters most to our organizations: improving every step of the healthcare experience. The Code also empowers you to fulfill our mission through your own ethical actions, making daily choices that align with our Code, our policies, and the law. Being a part of the Judi Health teams means never compromising on our Values, using good judgment and letting the Code guide us each day.

Turn to the Code often and seek help from any of the resources listed if you're ever unsure of the right thing to do. And if you think something may be violating our Code, speak up right away. That's how we protect our reputation and preserve our culture of integrity. We have an extraordinary opportunity before us—to deliver enduring social change and the efficient, accessible healthcare we all deserve.

By keeping that goal in sight and remaining committed to excellence and integrity, we can make the world a better, healthier place.

Anthony J. Loiacono
Chief Executive Officer
Judi Health

"TRULY GREAT COMPANIES ARE BUILT ON A FOUNDATION OF INTEGRITY."

A Message From Our Chief Compliance Officer

Truly great companies are built on a foundation of integrity. At Judi Health, we've worked hard to build a company and a culture that celebrates integrity and reflects our high standards in everything we do. That's the way we will always work—today and into the future.

Every day, Judi Health workforce members are focused on creating value for our customers, clients, and members and earning their trust. The decisions we make (no matter how small) have the power to build that trust or break it down. That's why we have our Code of Conduct—to unite us in our commitment to integrity and guide us to do the right things for our customers, clients, members, Company, and each other.

We ask that you do more than just read the Code—live it in your daily work. Apply it to your every action, especially when work gets complicated. You'll find the Code to be an invaluable tool, not only as a guide to making good decisions, but also when you believe our Code, policies, or laws have been broken. The Code shows you how to share your concerns.

Thank you for continuing to put your very best into everything we do. Together, we'll build lasting relationships and lasting success for our Company.

Lloyd D. Fiorini
General Counsel, Chief Compliance Officer
Judi Health

Purpose and Overview

Healthcare, and the technology behind it, never stops changing. At Judi Health, we welcome that change. In fact, we're an integral part of it, bringing transparency and efficiency to the PBM industry and ultimately, improving healthcare outcomes.

People and their care are central to all we do. They are why we go to work each day. Keeping them in mind keeps us focused on our mission and on doing what's right. We expect our workforce members to share this focus and embrace our shared responsibilities. That's how we build trust—in a spirit of service, accountability, and integrity.

That's exactly what this Code of Conduct is designed to do. It's your resource for:

- Promoting integrity and the highest standards of ethical conduct.
- Addressing common ethical situations you could encounter in your work.
- Finding help when you need it.
- Avoiding the appearance of anything improper in connection with our business activities.

Key Terms

Throughout the Code, you'll see these terms used:

Company
Judi Rx, Inc. and all its divisions and subsidiaries, including Judi Health, LLC (hereinafter referred to as "Judi Health").

Workforce Members
Refers to Company employees, volunteers, trainees, consultants, and other persons whose conduct, in the performance of work for the Company, are under the direct control of the Company, whether or not they are paid by the Company.

FDR
Refers to First Tier, Downstream, and Related Entities.

PBM
Refers to Pharmacy Benefit Managers, who manage prescription drug plan benefits for insurers and employers.

Complying with Laws and Regulations

Our Company is committed to compliance with all laws, rules, and regulations that apply to our business. It is impossible to anticipate every question you may have or situation you might face so, in addition to the Code, we also have other resources that can be of help. These additional resources are listed throughout the Code. As always, we rely on you to use good judgment and seek help when you need it. We do not operate in multiple countries.

Who Must Follow This Code

All workforce members of the Company, including executives, corporate officers, and members of our Board of Directors, are required to read, understand, and follow our Code. Consultants, contractors, agents, suppliers, First Tier, Downstream, Related Entities (FDRs), and temporary workforce members ("business partners") who serve as an extension of the Company are also expected to follow the spirit of our Code, as well as any applicable contractual provisions. If you supervise our business partners, you are responsible for communicating our standards and ensuring they are understood. If a business partner fails to meet our ethics and compliance expectations or their contractual obligations it may result in the termination of their contract.

Accountability and Discipline

Violating our Code, our policies, or the law, or encouraging others to do so, exposes our Company to liability and puts our reputation at risk. If you see or suspect a violation, **REPORT IT**. Anyone who violates our Code will be subject to disciplinary action, up to and including termination of their employment with the Company. Violations of laws or regulations may also result in legal proceedings and penalties including, in some circumstances, criminal prosecution.

Learn More

CRX.COMPL.001 Corporate Compliance Policies and Standards of Conduct

Purpose and Overview

The Company is committed to having an effective Corporate Compliance Program based on applicable laws, regulations, accreditation requirements, certifications, client contracts, and other guidance. Our Corporate Compliance Program includes internal controls that support all of us in completing tasks in a compliant and ethical manner. These controls are set up to help reduce or eliminate noncompliance, including potential **fraud, waste, or abuse (FWA)**, within the Company.

This Code of Conduct is the underlying framework for our corporate compliance program. We have a dedicated Chief Compliance Officer who is responsible for the oversight and implementation of the corporate compliance program. The Chief Compliance Officer provides regular status reports to the Corporate Compliance Committee and Board of Directors.

We are all expected to participate in and support the Corporate Compliance Program as necessary.

Our Responsibilities

Each of us has an obligation to act with integrity, even when this means making difficult choices. Meeting this obligation is what helps us succeed and grow.

Workforce Member Responsibilities

Each of us has a responsibility to:

- Act professionally, honestly, and ethically when conducting business on behalf of our Company.
- Know the information in our Code and Company policies, paying particular attention to the topics that apply to our specific job responsibilities.
- Complete all required workforce member training on time, and stay up-to-date on current standards and expectations.
- Report concerns about possible violations of our Code, our policies, or the law to your manager, an executive, or any of the resources listed in this Code.
- Cooperate and tell the truth when responding to an investigation or audit, and never alter or destroy records in response to an investigation or when an investigation is anticipated.

Additional Responsibilities of Managers

Managers are expected to:

- Lead by example. Model high standards of ethical business conduct, and help create a work environment that values mutual respect and open communication.
- Be a resource for others. Communicate often with workforce members and business partners about how the Code and other policies apply to their daily work.
- Be proactive. Look for opportunities to discuss and address ethical dilemmas and challenging situations with others.
- Delegate responsibly. Never delegate authority to any individual whom you believe may engage in unlawful conduct or unethical activities.
- Respond quickly and effectively. When a concern is brought to your attention, treat it seriously and with respect for everyone involved.
- Be aware of the limits of your authority. Do not take any action that exceeds your authority. If you are ever unsure of what is appropriate (and what is not), discuss the matter with your manager.

Remember: No reason, including the desire to meet business goals, should ever be an excuse for violating our Code, our policies, or the law.

Purpose and Overview

Our Responsibilities

What If?

I'm a manager and not clear about what my obligations are if someone comes to me with an accusation—and what if it involves a senior manager?

No matter who the allegation involves, you must **REPORT IT**. *Our Company provides several options for reporting concerns. If for any reason you are uncomfortable making a report to a particular person, you may talk to any of the other resources listed in the Code.*

I observed misconduct in an area not under my supervision. Am I still required to report the issue?

You are primarily responsible for workforce members and business partners under your supervision, but all workforce members are required to report misconduct. As a leader, you have a special obligation to be proactive. The best approach would be to talk first with the manager who oversees the area where the problem is occurring, but if this isn't feasible or effective, you should contact another resource described in our Code.

Learn More

CRX.COMPL.004c Reporting Compliance Program Noncompliance

Our Guidelines for Good Decision Making

Making the right decision is not always easy. There may be times when you'll be under pressure or unsure of what to do. Always remember that when you have a tough choice to make, you are not alone. There are resources available to help you.

Facing a Difficult Decision? It may help to ask yourself:

Is it legal? → **Is it consistent with our Code and our Values?** → **Would I feel comfortable if senior management and others in the Company knew about it?** → **Would I feel comfortable if my decision or my actions were made public?**

If the answer to all of these questions is "**yes**," the decision to move forward is probably okay, but if the answer to any question is "**no**" or "**I am not sure**," stop and seek guidance.

Remember, in any situation, under any circumstances, it is always appropriate to ask for help.

One More Thing …

We value your feedback. If you have suggestions for ways to enhance our Code, our policies, or our resources to better address a particular issue, bring them forward. Promoting an ethical Company is a responsibility we all share.

Learn More

CRX.COMPL.001 Corporate Compliance Policies and Standards of Conduct

Speaking Up and Reporting Concerns

If you see or suspect a violation of our Code, our policies, or the law, or if you have a question about what to do, talk to your manager.

If you are uncomfortable speaking with your manager, there are other resources available to help you:

— Contact another member of management.

— Contact **Human Resources**

— Contact the Anonymous Hotline:

- **Website: Mitratech**
- **Toll-Free Telephone:**
  - » USA & Canada (all languages): 855-222-0934
  - » Mexico (Spanish): 800-461-1552

What If?

I believe someone misused the Hotline, by making an anonymous call and falsely accusing someone of wrongdoing. What should I do?

Report your concern immediately. Experience has shown that the Hotline is rarely used for malicious purposes, but it is important to know that we will follow up on reports, and anyone who uses the Hotline in bad faith to spread falsehoods or threaten others, or with the intent to damage another person's reputation, will be subject to disciplinary action.

What to Expect When You Use the Hotline

The Hotline web portal and phone line are available 24 hours a day, seven days a week. Operated by an independent third-party provider of corporate compliance services, the Hotline will document your concerns in detail and forward them to the Company for further investigation.

When you contact the Hotline, you may choose to remain anonymous where permitted by local law. All reports received will be treated equally, whether they are submitted anonymously or not.

After you make a report, you will receive an identification number so you can follow up on your concern. Following up is especially important if you have submitted a report anonymously, as we may need additional information to conduct an effective investigation. This identification number will also enable you to track the resolution of the case; however, please note that out of respect for privacy, we will not be able to inform you about individual disciplinary actions.

Any report you make will be kept confidential by all individuals involved with reviewing and, if necessary, investigating it.

Remember, an issue cannot be addressed unless it is brought to someone's attention.

Learn More

CRX.COMPL.004c Reporting Compliance Program Noncompliance

Speaking Up and Reporting Concerns

Our Commitment to Non-retaliation

The Company strictly prohibits and does not tolerate retaliation against anyone for reporting potential noncompliance in good faith, being involved with an investigation of noncompliance, or participating in the Corporate Compliance Program.

Examples of protected activities include, but are not limited to:

- Conducting self-evaluations
- Participating in audits and/or monitoring activities
- Performing remedial actions
- Participating in Corrective Action Plans (CAPs)
- Reporting potential compliance risks
- Identifying and reporting noncompliance, including self-reporting

All forms of retaliation are prohibited, including any form of adverse action, discipline, threats, intimidation, or other form of retaliation. No one may seek revenge against or try to “get even” with anyone, regardless of who is implicated.

What Does Reporting “in Good Faith” Mean?

It means making a genuine attempt to provide honest, complete, and accurate information, even if it later proves to be unsubstantiated or mistaken.

What If?

I suspect there may be some unethical behavior going on in my business unit involving my manager. I know I should report my suspicions, and I am thinking about using the Hotline, but I am concerned about retaliation.

You are required to report misconduct and, in your situation, using the Hotline is a good option. We will investigate your suspicions and may need to talk to you to gather additional information. After you make the report, if you believe you are experiencing any retaliation, **REPORT IT**. *We take claims of retaliation seriously. Reports of retaliation will be thoroughly investigated and, if they are true, retaliators will be disciplined.*

Learn More

CRX.COMPL.004d Non-retaliation

Speaking Up and Reporting Concerns

Disciplinary Standards and Corrective Action

As we perform our jobs, we must remain compliant with applicable laws, regulations, accreditation requirements, certifications, and other guidance and are expected to comply with the Company's values, policies and procedures, and Code of Conduct.

Failure to do so may result in corrective action, including:

- Performance counseling or re-training
- Warnings (verbal, written and final written warnings)
- Performance improvement plan
- Suspension
- Termination

Corrective action does not need to be taken in any particular order and may include any or all of the actions listed above.

The Company sanctions anyone, regardless of their job title or level within the organization, for participating in, encouraging, directing, facilitating, or permitting noncompliance.

We are committed to fairly and consistently issuing appropriate corrective action to address noncompliance and deter future noncompliance.

Staying Safe and Healthy at Work

Ensuring safety is an integral part of everything we do. Reporting risks and hazards is not just the right thing to do, it's a requirement, because a failure to speak up about an incident, or to participate in an investigation into an incident, can have serious repercussions for our Company, and for every workforce member on the job, every day.

Each of us is responsible for acting in a way that protects ourselves and others. No matter what job you do or where you do it, we count on you to actively promote a safe and healthy workplace, and report any situations that may pose a health, safety, or security risk. Do your part to keep everyone in the Judi Health family injury-free.

Alcohol and Drugs

While at work or on Company business:

- Ensure you are always prepared to carry out your work responsibilities and never do so impaired by drugs (including lawfully prescribed drugs).
- Never use, possess, sell, exchange, or purchase alcohol, drugs, or illegal substances.
- Be aware, the Company may require drug or alcohol testing if it reasonably suspects a workforce member is impaired.

Workplace Violence

Violence of any kind has no place at our Company. We won't tolerate:

- Intimidating, threatening, or hostile behavior.
- Causing physical injury to another.
- Acts of vandalism, arson, sabotage, or other criminal activities.
- The carrying of firearms or other weapons onto Company property unless you are authorized to do so.

Staying Safe and Healthy at Work

Do the Right Thing

- Follow the safety, security, and health rules and practices that apply to your job.
- Maintain a neat, safe working environment by keeping workstations, aisles, and other workspaces free from obstacles, wires, and other potential hazards.
- Notify your manager immediately about any unsafe equipment, or any situation that could pose a threat to health or safety or the environment. As a workforce member, you have the right and the responsibility to stop any work if you feel your safety is at risk.
- Cooperate with any investigations into incidents.

Watch Out For

- Unsafe practices or work conditions.
- Carelessness in enforcing security standards, such as facility entry procedures and password protocols.

What If?

I've noticed some practices in my area that don't seem safe. Who can I speak to? I'm new here and don't want to be considered a troublemaker.

Discuss your concerns with your manager or **Human Resources**. *There may be very good reasons for the practices, or you may be bringing to light an issue that needs to be addressed. In either case, raising a concern about safety does not make you a troublemaker. It makes you a responsible workforce member who is concerned about the safety of others.*

A subcontractor commits a violation of our standards. Are subcontractors expected to follow the same health, safety, and security policies and procedures as workforce members?

Absolutely. Managers are responsible for ensuring that subcontractors and other business partners at work on Company premises understand and comply with all applicable laws and regulations, as well as with additional requirements our Company may have.

Providing Equal Opportunities

Our Company helps bring together workforce members with a wide variety of backgrounds, skills, and cultures. Combining such a wealth of talent and resources creates the diverse and dynamic teams that consistently drive our results. We are committed to ensuring that everyone in our workplace—workforce member, job applicants, and business partners—feel welcome and valued and are given opportunities to grow, contribute, and develop with us. To uphold that commitment, we support laws prohibiting discrimination and provide equal opportunity for employment, income, and advancement in all our departments, programs, and worksites.

If you are responsible for making employment decisions on behalf of the Company, base your decision-making on qualifications, demonstrated skills, and achievements—and never on race, color, religion, sex (including pregnancy, sexual orientation, or gender identity), national origin, age, disability, genetic information, or any other characteristic protected by law.

Do the Right Thing

- Treat others respectfully and professionally.
- Promote diversity in hiring and other employment decisions.
- Do not discriminate against others on the basis of any other characteristic protected by law or Company policy.

Watch Out For

- Comments, jokes, or materials, including emails, which others might consider offensive.
- Inappropriate bias when judging others. If you supervise others, judge them on performance. Use objective, quantifiable standards and avoid introducing unrelated considerations into your decisions.

What If?

One of my coworkers sends emails containing jokes and derogatory comments about certain nationalities. They make me uncomfortable, but no one else has spoken up about them. What should I do?

You should notify your manager or **Human Resources**. *Sending these kinds of jokes violates our Values, our email usage policies, and our standards on diversity, harassment, and discrimination. By doing nothing, you are condoning discrimination and tolerating beliefs that can seriously erode the team environment we have all worked to create.*

Learn More

CRX.HR.004 Hiring and Onboarding

Preventing Harassment

We all have the right to work in an environment that is free from intimidation, harassment, bullying, and abusive conduct. The Company does not tolerate verbal or physical conduct by any workforce member that harasses another, disrupts another's work performance, or creates an intimidating, offensive, abusive, or hostile work environment.

If you see, suspect, or feel you have been the victim of harassment (including sexual harassment), **REPORT IT** immediately. You'll be helping to preserve a respectful and productive workplace.

Sexual Harassment

A common form of harassment is sexual harassment, which in general occurs when:

- Actions that are unwelcome—such as a request for a date, a sexual favor, or other similar conduct of a sexual nature—are made a condition of employment or used as the basis for employment decisions.
- An intimidating, offensive, or hostile environment is created by unwelcome sexual advances, insulting jokes, or other offensive verbal or physical behavior of a sexual nature.

Learn More

For Consensual Relationships, see the CRX.HR.014 Dating Policy

Preventing Harassment

Do the Right Thing

- Promote a positive attitude—support policies designed to build a safe, ethical, and respectful workplace.
- Help each other—speak out when a coworker's conduct makes others uncomfortable.
- Be professional—do not visit inappropriate internet sites or display sexually explicit or offensive pictures.
- Speak up—report all incidents of harassment and intimidation that may compromise our ability to work together and be productive.

Watch Out For

- Threatening remarks, obscene phone calls, stalking, or any other form of harassment.
- Sexual harassment or other unwelcome verbal or physical conduct of a sexual nature.
- The display of sexually explicit or offensive pictures or other materials.
- Sexual or offensive jokes or comments.
- Verbal abuse, threats, or taunting.

What If?

While on a business trip, a colleague of mine repeatedly asked me out for drinks and made comments about my appearance that made me uncomfortable. We weren't in the office, and it was after regular working hours, so I wasn't sure what I should do. Was that harassment?

It could be. We expect our workforce members to practice respect, not only during working hours but in all work-related situations, including business trips. Tell your colleague you are uncomfortable with these actions and ask them to stop. If they continue, report the problem.

I frequently hear a colleague making derogatory comments to another coworker. These comments make me feel uncomfortable, but I feel like it's none of my business, and the person they're directed at will speak up if they are offended. Should I ignore this?

No, you shouldn't. It's up to each of us to help maintain a work environment where people feel welcome, valued, and included. Since you're aware of this situation, you have a responsibility to speak up about it. If you feel you can, speak to your colleague and ask that this behavior stop. If you feel you can't or the comments continue, talk to your manager or another resource.

Using Our Physical and Electronic Assets

Our Company entrusts workforce members with assets (both tangible and intangible) that enable us to operate. Physical assets include Judi Health facilities, materials, and equipment. Electronic assets include computer and communication systems, software, and hardware. Files and records are also Company assets, and we have a responsibility to ensure their confidentiality, security, and integrity.

Each of us is personally responsible for using these assets with care. Your personal use of Company assets is discouraged, but where permitted, should be kept to a minimum and have no adverse effect on productivity and the work environment. Please note any information you create, share, or download onto Company systems is the property of Judi Health. We reserve the right to access, review, and monitor system usage at any time, without prior notice, to the extent permitted by applicable law.

Remote Working

Although more workforce members are working remotely than ever before, our responsibilities to the Company remain the same. No matter where we are working—at home, in a café, or anywhere else in the world—we have a duty to maintain our Company's high standards and follow our policies.

If you work remotely, always do what is expected of you. Follow the same practices and put in the same number of hours and level of effort you would in an office setting. Also protect any Company assets that are in your care, including technology, hardware, and information. Be available to your colleagues during regular work hours and do what is right and required, even without direct supervision.

Do the Right Thing

— Use Company assets to carry out your job responsibilities, never for activities that are improper or illegal.

— Observe good physical security practices, especially those related to badging in and out of our facilities.

— Be a good steward of our electronic resources and systems, and practice good cybersecurity:

- Do not share passwords or allow other people, including friends and family, to use Company assets.
- Only use software that has been properly licensed. The copying or use of unlicensed or "pirated" software on Company computers or other equipment to conduct Company business is prohibited. If you have any questions about whether or not a particular use of software is licensed, contact the **IT Department**.
- Lock your workstation when you step away and log off our systems when you complete your work for the day.
- Beware of phishing attempts—use caution in opening email attachments from unknown senders or clicking on suspicious links.

Watch Out For

— Requests to borrow or use Company equipment without prior approval.

— Excessive use of Company resources for personal purposes.

— Unknown individuals without proper credentials entering our facilities.

Learn More

CRX.IT.030 Asset Management

CRX.IT.010 Facility Access

Preserving Private Data

We respect the personal information of others. We follow our policies and all applicable laws and regulations in collecting, accessing, using, storing, sharing, and disposing of sensitive information.

Make sure you know the kind of information that is considered personal information. It includes anything that could be used to identify someone, either directly or indirectly, such as a name, email address, phone number, or credit card number. Only use personal information, or share it with others outside the Company, for legitimate business purposes.

Immediately report potential inappropriate disclosures of **confidential, proprietary, and non-public information**. If the disclosure contained PHI or PII, also contact the **Privacy Department**.

Watch Out For

— Failing to shred or securely dispose of sensitive information.

— Using “free” or individually purchased internet hosting, collaboration, or cloud services that could put personal information at risk.

Learn More

CRX.PRIVACY.005 Restrictions on Use and Disclosure of PHI and Confidential Communications

Implementing Artificial Intelligence

We embrace new technologies, including Artificial Intelligence (AI), which is rapidly changing the way our Company collects, uses, and analyzes data. AI is also empowering us to give customers, clients, and members more efficient and personalized experiences.

Protect the security of our systems, as well as our intellectual property and confidential information, including any client or member data. Only utilize AI tools that have been approved for use by the Company and do so consistently with our AI Use policy. When working with sensitive or proprietary data in AI, you should use the minimum data necessary for the purpose. When in doubt, consult with the **IT Security and Privacy Department**.

Do the Right Thing

- Maintain human oversight at all stages of AI use.
- Avoid AI tools and uses that could create or spread bias, discrimination, or unfair outcomes.
- Verify the accuracy of AI outputs and reference source material to minimize outdated or unreliable information.
- Protect intellectual property and confidential information, customer/client/member data, and the security of our systems—never input proprietary data into an AI tool without prior approval from **IT Security**.

Learn More

CRX.ITSC.013 AI Use Policy

Interacting with Healthcare Professionals

We put patients first. In our interactions with healthcare professionals, we promote patient welfare by observing good business practices, meeting industry standards, and complying with Company policies. We also comply with federal and state laws that govern our relationships with healthcare professionals, including the U.S. Anti-kickback Statute and the Stark Law.

Make sure all interactions are professional and serve a legitimate business purpose, and never engage in any conduct that is intended to—or could even suggest the appearance of—improperly influencing a healthcare professional's decision.

Do the Right Thing

— Never pay or offer to pay anyone, including colleagues, physicians, or any other provider to refer a patient. If you are offered any kind of payment for a patient referral, turn it down.

— Do not offer or give anything of value to influence or reward prescribing, using, purchasing, leasing, or recommending certain products or services.

Watch Out For

— **Gift-giving**—federal and state laws and our policies strictly limit what we may give healthcare providers in terms of gifts, entertainment, promotional items, and other hospitality and business courtesies.

— **Improper influence**—don't interfere with a healthcare professional's independent judgment.

Learn More

CRX.COMPL.012 Business Courtesies

Vendor Management

Our vendors are an extension of our Company. We engage third parties in ways that uphold our commitment to integrity, compliance, and excellence. You must follow the Vendor Management process via our Vendor Management System (Tropic). This process ensures we consistently establish, maintain, renew, and update third-party relationships on time and in compliance with applicable policies and laws.

Do the Right Thing

Use the Vendor Management process before:

— Onboarding a new vendor.

— Renewing or modifying an agreement.

— Terminating services.

The Vendor Management process includes:

— Coordinated review with Legal, Compliance, IT Security, and Finance.

— Risk evaluation to ensure appropriate contractual protections.

— Confirmation of data privacy safeguards.

— Term alignment for payment and performance.

When selecting vendors, keep the following criteria in mind:

— Focus on the ability to meet business needs and technical requirements objectively.

— Negotiate agreements in good faith; ensure fairness and reasonableness for both parties.

— Avoid conflicts of interest and maintain transparency in all vendor dealings.

Working with the Government

We are committed to meeting the many special legal, regulatory, and contractual requirements that apply to our government contracts. These requirements may apply to bidding, accounting, invoicing, subcontracting, employment practices, contract performance, gifts and entertainment, purchasing, and other matters. These requirements may also flow down to individuals and companies working on our behalf.

If you are responsible for conducting business with the government on behalf of the Company, make sure you know and comply with what's contractually required as well as all laws and regulations that apply to our government-related work.

Do the Right Thing

- Comply with all legal, regulatory, and contractual requirements for government contracts.
- Understand obligations related to bidding, accounting, invoicing, subcontracting, and employment practices.
- Never offer gifts or anything of value to influence government decisions; follow strict compliance rules.

Giving Gifts Responsibly

A modest gift may be a thoughtful "thank you," or a meal may offer an opportunity to discuss business. If not handled carefully, however, the exchange of gifts and entertainment could be improper or create a conflict of interest. This is especially true if an offer is extended frequently, or if the value is large enough that someone may think it is being offered in an attempt to influence a business decision.

Only offer and accept gifts and entertainment that comply with our policies, and make sure that anything you give or receive is accurately reported in our books and records.

Do the Right Thing

- Only provide and accept gifts and entertainment that are reasonable complements to business relationships.
- Make sure anything given or received complies with the Company policies of both the giver and the recipient.
- Raise a concern whenever you suspect that a colleague or business partner may be improperly attempting to influence a decision of a customer or government official.
- Follow our policy, which requires workforce members to never:
  - Accept or make any offer that might compromise fair decision-making or influence business relationships (or gives the appearance of either).
  - Give, receive, or ask for business courtesies in return for business.
  - Receive gifts of cash or cash equivalents (e.g. gift cards) in any amount.
  - Give or receive business courtesies to or from members, prescribers, pharmacies, pharmaceutical manufacturers, or U.S. or foreign government employees or officials, including those of government owned businesses.

Government Officials

Be aware that the rules for what we may give to—or accept from—government officials are much more strict. Don't offer anything of value to a government official without obtaining approval, in advance, from the **Compliance Department**. And remember: We do not accept or provide gifts, favors, or entertainment to anyone—even if it complies with our policies—if the intent is to improperly influence a decision.

Giving Gifts Responsibly

Watch Out For

- Situations that could embarrass you or our Company (e.g., entertainment at sexually oriented establishments).
- Gifts, favors, or entertainment that may be reasonable for a privately owned company but not for a government official or agency.

What If?

When traveling, I received a gift from a business partner that I believe was excessive. What should I do?

You need to let your manager know and report it to the **Compliance Department** *as soon as possible. We may need to return the gift with a letter explaining our policy. If a gift is perishable or impractical to return, another option may be to distribute it to workforce members or donate it to charity, with a letter of explanation to the donor.*

Learn More

CRX.COMPL.012 Business Courtesies

Avoiding Conflicts of Interest

A conflict of interest can occur whenever a workforce member has an interest or activity that may interfere with their ability to make an objective decision on behalf of the Company. Conflicts of interest may be actual, potential, or even just a matter of perception.

Each of us is expected to use good judgment and avoid situations that can lead to even the appearance of a conflict, because the perception of a conflict can undermine the trust others place in us and damage our reputation. Conflict of interest situations are not always clear-cut, so any potential conflict must be reported to the **Compliance Department** for review.

Do the Right Thing

- Avoid conflict of interest situations whenever possible.
- Always make business decisions in the best interest of the Company.
- Think ahead and proactively address situations that may put your interests or those of a family member in conflict with our Company.
- Discuss with your manager full details of any situation that could be perceived as a potential conflict of interest.

Learn More

CRX.COMPL.011 Conflicts of Interest

Potential Conflicts of Interest

Be alert to situations, including the following, which are common examples of potential conflicts of interest:

Corporate opportunities

If you learn about a business opportunity because of your job, it belongs to our Company first. This means that you should not take that opportunity for yourself unless you get approval from the Compliance Officer.

Friends and relatives

On occasion, it is possible that you may find yourself in a situation where you are working with a close friend or relative who works for a customer, business partner, competitor, or even our Company. Since it is impossible to anticipate every scenario that could create a potential conflict, you should disclose your situation to your manager to determine if any precautions need to be taken.

Outside employment

To ensure that there are no conflicts and that potential issues are addressed, please reference CRX.COMPL.011 Conflicts of Interest. If approved, make sure the outside activity does not interfere or compete with your work at our Company. Working for a competitor, business partner, or customer may raise conflicts that will need to be resolved.

Personal investments

A conflict can occur if you have a significant ownership or other financial interest in a competitor, business partner, or customer. Make sure you know what's permitted—and what's not—by our policies and seek help with any questions.

Civic activities

Unless Company management specifically asks you to do so, you shouldn't accept a seat on the board of directors or advisory board of any of our competitors, business partners, or customers, especially if your current job gives you the ability to influence our relationship with them.

Keeping Accurate Records

The accuracy and completeness of our business records and financial disclosures are essential to making informed decisions and supporting investors, regulators, and others. Our books and records must accurately and fairly reflect our transactions in sufficient detail and in accordance with our accounting practices and policies.

Some workforce members have special responsibilities in this area, but all of us contribute to the process of recording business results or maintaining records. Ensure that any information you record is accurate, timely, complete, and maintained in a manner that is consistent with our internal controls, disclosure controls, and legal obligations.

Do the Right Thing

- Create business records that accurately reflect the truth of the underlying event or transaction. Be guided by the principles of transparency and truthfulness.
- Write carefully in all business communications. Write as though someday the records you create may become public documents.
- Place business records and data in approved storage locations.
- Save business records in an approved collaboration application (SharePoint).
- Save data to an access-protected department folder.
- Maintain required paper records at the Company facility.

Watch Out For

- Unclear or incomplete records that obscure the true nature of any action.
- Undisclosed or unrecorded funds, assets, or liabilities.
- Improper destruction or disposal of documents or paper records.
- Storage of in-progress work on unapproved cloud platforms or external websites.
- Business records and data saved to public folders.

Records Management

Documents should only be disposed of in compliance with Company policies and should never be destroyed or hidden. You must never conceal wrongdoing or permit others to do so. Never destroy documents in response to—or in anticipation of—an investigation or audit.

If you have any questions or concerns about retaining or destroying corporate records, please contact the **Legal Department**.

What If?

At the end of the last quarter reporting period, my manager asked me to record additional expenses, even though I had not yet received the invoices from the supplier and the work has not yet started. I agreed to do it, since we were all sure that the work would be completed in the next quarter. Now I wonder if I did the right thing.

No, you didn't. Costs must be recorded in the period in which they are incurred. The work was not started, and the costs were not incurred by the date you recorded the transaction. It was therefore a misrepresentation and, depending on the circumstances, could amount to fraud.

Learn More

CRX.LEGAL.009 Document Production and Retention

Protecting Confidential Information and Intellectual Property

The Company's confidential and proprietary information is important to our business. We are expected to protect our confidential and intellectual property from theft, misuse, and improper disclosure. Be vigilant and protect this information, always assuming that all Company information is confidential, proprietary, and non-public.

Because our customers, clients, members, and business partners place their trust in us, we must protect their confidential information just as we protect our own. Be aware that your obligation to protect confidential information and intellectual property continues even after your employment with the Company ends.

Types of Information

Confidential Information
Any information related to business operations which cannot be learned outside of that business. Confidential information exists in all forms (e.g., written, spoken, observed, electronic). Our own health information, performance reviews, corrective actions, and any other personally identifiable information (PII) that is not available to the public, is also considered confidential information.

Proprietary Information
Any information developed, created, or discovered by the Company. This also includes any information which became known by, or was conveyed to our Company, which has commercial value in our business. Proprietary information can include secret system coding, internal detailed processes, future projects or clients, methods used in Company production, or other trade secrets.

Non-public Information Includes information about:

- Our Company and its business.
- Current or prospective investors, clients, and owners.
- Members, claims, or providers.
- All other private records, documents, electronic communications, or other information that is confidential or proprietary.

Personally Identifiable Information (PII)
Information that identifies, or could be used to identify an individual, either by itself or when combined with other information.

Protected Health Information (PHI)
Information that is created or received by a healthcare provider (including a pharmacy), health plan, employer, or healthcare clearinghouse that relates to the:

- Past, present, or future physical or mental health or condition of an individual
- Provision of healthcare to an individual.
- Past, present, or future payment for the provision of healthcare to an individual, and either identifies or could be used to identify the individual.

PHI and PII may include national identification numbers (such as Social Security numbers), dates of birth, financial and medical information, and other information that identifies or relates to a particular individual. PHI may include claim information, records regarding payment for care, or information such as a member's telephone number if we received it from a health plan. Contact the **Privacy Department** to report inappropriate, potential or unauthorized access, use, or disclosure of PHI or PII upon discovery.

Protecting Confidential Information and Intellectual Property

Do the Right Thing

— Only access, use, or disclose the minimum amount of information necessary to do your job.

— Only share confidential information with those who are authorized, on a "need to know" basis and only for legitimate business purposes.

— Never leave confidential, proprietary, or non-public information in a place where unauthorized people have access to it. Keep it stored on Company information systems.

— Lock your computer when leaving it unattended.

— Disclose to the Company any IP that you create during your employment and return confidential, proprietary, and non-public information in your possession upon leaving the Company.

— Remove any unnecessary data or non-requested information from reports before sending it to others.

Watch Out For

— Discussions of Company confidential information in places where others might be able to overhear—for example on planes and elevators, in restaurants, and when using your phone.

— Sending confidential information to unattended devices or printers.

— Requests from business partners for confidential information about our customers, clients, and workforce members or about other business partners, if there is no associated business requirement or authorization.

— Unintentional exposure of confidential information or intellectual property—notify your manager immediately.

Learn More

CRX.PRIVACY.005 Restrictions on Use and Disclosure of PHI and Confidential Communications

Intellectual Property

Examples of intellectual property (IP) include:

- Business and marketing plans
- Company initiatives (existing, planned, proposed, or developing)
- Customer, client, or member lists
- Trade secrets and discoveries
- Methods, know-how, and techniques
- Innovations and designs
- Systems, software, and technology
- Patents, trademarks, and copyrights

Our Company commits substantial resources to technology development and innovation, and the creation and protection of our intellectual property rights are critical to our business. Contact the **Legal Department** if you receive questions regarding:

- The scope of our intellectual property rights
- How our Company rights apply to another company's products
- How a third party's intellectual property rights apply to our Company's intellectual property rights or products

Protecting Confidential Information and Intellectual Property

Confidential Information of Others

Our customers, clients, members, and business partners place their trust in us. We must protect their confidential information just as we protect our own. Make sure you understand the expectations of customers and business partners regarding the protection, use, and disclosure of the confidential information that they provide to us.

Do the Right Thing

— Limit any access to third-party confidential information to those who have a need to know in order to do their job, and only for authorized purposes.

— Immediately report any loss or theft of confidential information to your manager.

Watch Out For

— Requests by business partners for confidential information about our customers/clients/members or about other business partners if there is no associated business requirement or authorization.

— Unintentional exposure of confidential information about our customers, clients, workforce members, or business partners in public settings or through unsecure networks.

Fighting Fraud, Waste, and Abuse

Our Company is committed to the integrity of the healthcare system and to detecting, correcting, and preventing false claims. As part of this commitment, we expect our workforce members to be able to recognize and report instances of **fraud**, **waste**, and **abuse**.

Each of us has a responsibility to ensure payments and transactions are properly authorized and fully and accurately recorded in compliance with all applicable laws and Company policies.

Key Definitions

Abuse
Involves payment for items or services when there is no legal entitlement to that payment, and the provider has not knowingly and/or intentionally misrepresented facts to obtain payment.

Fraud
Knowingly and willfully executing, or attempting to execute, a scheme or artifice to defraud any healthcare benefit program or to obtain (by means of false or fraudulent pretenses, representations, or promises) any of the money or property owned by, or under the custody or control of, any healthcare benefit program.

Waste
Includes the overutilization of services, or other practices that, directly or indirectly, result in unnecessary costs to the Medicare program. Waste is generally not considered to be caused by criminally negligent actions but rather the misuse of resources.

Do the Right Thing

- Complete all required training and know the definitions of “fraud,” “waste,” and “abuse.”
- Ensure timely and accurate documentation, coding, and billing that reflect services ordered and actually performed.
- Only bill for services we actually provide.
- Promptly report any instances of suspected fraud, waste, or abuse.

Watch Out For

Activities that constitute fraud, waste, or abuse, such as:

- Billing for services, procedures, or supplies that have not actually been provided.
- Providing services to patients that are not medically necessary.
- Forging a physician’s signature to obtain pharmaceuticals.
- Intentionally misrepresenting or manipulating information to receive payment for services that were not provided.
- Lack of supporting documentation, where it is required.

Learn More

CRX.COMPL.008 FWA Program

Communicating with the Public

We are committed to maintaining honest, professional, and lawful internal and external (i.e., public) communications. To achieve this, a consistent voice is required when providing information to the public or making disclosures. That is why only authorized persons may speak on behalf of the Company or our other service lines. This includes our C-suite and the service line leadership, but exceptions may be made and should be referred to **Marketing**.

Additionally, outside interview or speaking engagement requests should be screened to ensure that the inquiries from media (journalists, reporters, podcasters, bloggers, etc.), investors or securities analysts, or other third-parties (e.g., event coordinators) are appropriate. Our PR agency may assist with the evaluation of such requests to ensure that we are appropriately allocating our time and resources.

Watch Out For

- Giving public speeches or writing articles for professional journals or other public communications that relate to the Company without appropriate management approval.
- The temptation to use your title or affiliation outside of your work for the Company without it being clear that the use is for identification only.
- Invitations to speak "off the record" to journalists or analysts who ask you for information about the Company or its customers or business partners.

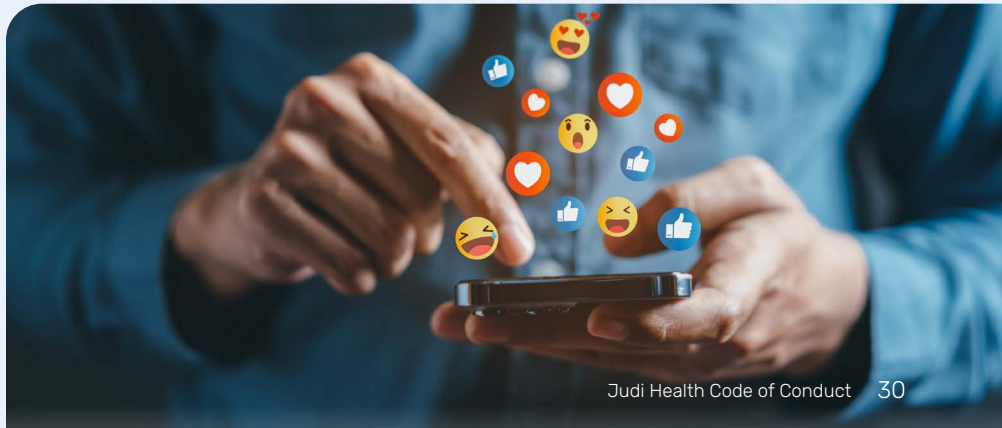
Social Media

Every communication about our Company affects our reputation and our brand, so we take care online. We must never post anything that would be considered harassing or discriminatory, and we must never breach confidential information about our Company, our workforce members, or our business partners.

If you participate in internet discussion groups, chat rooms, bulletin boards, blogs, social media sites, or other electronic communications, even under an alias, never give the impression that you are speaking on behalf of the Company. If you believe a false statement about our Company has been posted, do not respond, even if your intent is to "set the record straight." Your posting might be misinterpreted, start false rumors, or may be inaccurate or misleading. Instead, contact **Human Resources**.

Full, Fair, and Timely Disclosures

Our Company is committed to meeting its obligations of full, fair, and timely disclosure in all reports and documents that describe our business and financial results, and other public communications.



Proper Marketing Practices and Disclosures

Our advertising and promotion efforts focus on conveying useful information to healthcare providers, patients, customers, clients, and members.

Do your part to ensure our product claims are grounded in scientific evidence, accepted medical practice, and government-approved labeling rules.
Our communications and marketing strategies are designed to promote our brand in the best possible light while remaining compliant with all rules, regulations, and best practices (e.g., avoiding online conflicts and not engaging in dialogue that conflicts with our Values).

Following Anti-Corruption and Bribery Laws

Our Company is committed to complying with all applicable anti-corruption laws. We believe that all forms of bribery and other corrupt practices are an inappropriate way to conduct business regardless of local customs.

Do not pay or accept bribes or kickbacks, at any time for any reason. This applies equally to any person or company representing our Company. Our partners must understand that they are required to operate in strict compliance with our standards and to maintain accurate records of all transactions. Never ask them to do something that we are prohibited from doing ourselves.

Key Definitions

Bribery
Giving or receiving anything of value (or offering to do so) to obtain a business, financial, or commercial advantage.

Corruption
The abuse of an entrusted power for private gain.

Facilitation payments
Typically small payments to a low-level government official that are intended to encourage them to perform their responsibilities.

Government officials
Include government employees, political parties, candidates for office, employees of public organizations, and government-owned entities.

Do the Right Thing

- Understand the standards set forth under anti-bribery laws which apply to your role at the Company.
- Never give anything of value inconsistent with local laws and regulations to any government official. If you are not sure of the local laws, the safest course of action is to not give anything of value.
- Exercise due diligence and carefully monitor third parties acting on our behalf particularly when dealing in countries with high corruption rates and in situations where “red flags” would indicate further screening is needed.
- Accurately and completely record all payments to third parties.

Watch Out For

- Apparent violations of anti-bribery laws by our business partners.
- Agents who do not wish to have all terms of their engagement with the Company clearly documented in writing.

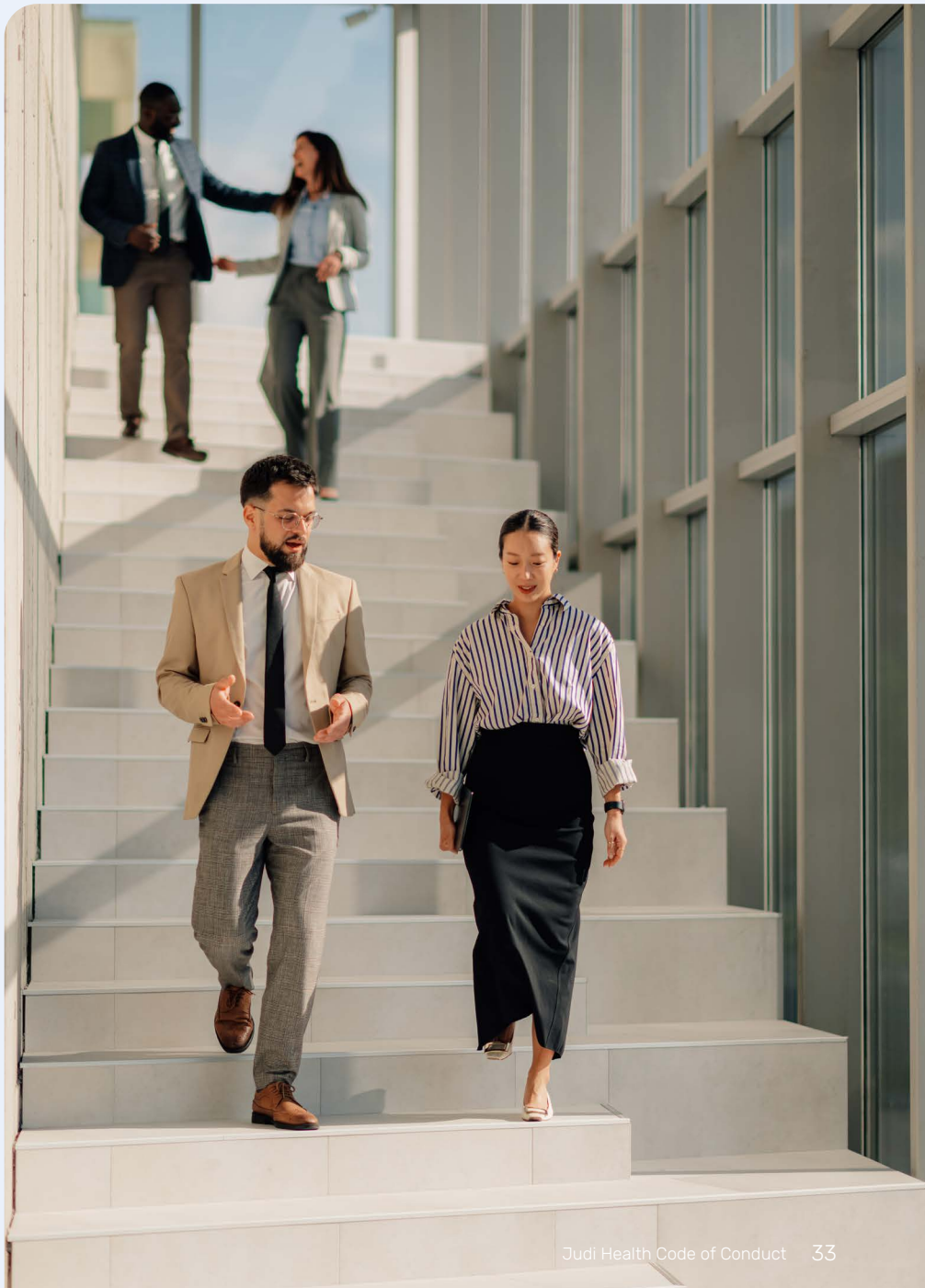
Understanding Money Laundering

Money laundering is a global problem with far-reaching and serious consequences. It is defined as the process of moving funds made from illegal activities through a legal business to make them appear legitimate. Involvement in such activities undermines our integrity, damages our reputation, and can expose our Company and the individuals involved to severe sanctions. We are committed to conducting business in a way that prevents money laundering and complying with all anti-money laundering, financial crimes, and anti-terrorism laws wherever we operate.

Be alert to the warning signs of money-laundering. Report any suspicious financial transactions and activities to the **Legal Department** and, if required, to appropriate government agencies.

Watch Out For

- Attempts to pay in cash or in a different currency than shown on the invoice.
- Requests to ship to a country that differs from where payment originated.
- Avoidance of recordkeeping requirements.
- Payments made by someone who is not a party to the transaction.
- Unusual changes to a customer's normal pattern of transactions.



Avoiding Insider Trading

We respect every company's right to protect its material, nonpublic ("inside") information, and we comply with insider trading laws.

In the course of business, you may learn confidential information about our Company or about other publicly traded companies that is not available to the public. Trading securities while aware of inside information, or disclosing it to others who then trade ("tipping"), is prohibited by various laws and our policies.

Do the Right Thing

— Do not buy or sell securities of any company when you have material nonpublic information about that company.

— Protect material nonpublic information from the general public including information in both electronic form and in paper copy.

— Discuss any questions or concerns about insider trading with the Legal Department.

Watch Out For

— Requests from friends or family for information about companies we do business with or have confidential information about. Even casual conversations could be viewed as illegal "tipping" of inside information.

— Sharing material nonpublic information with anyone, either on purpose or by accident, unless it is essential for Company-related business. Giving this information to anyone else who might make an investment decision based on your inside information is considered "tipping" and is against the law regardless of whether you benefit from the outcome of their trading.

Material Information

Material information is the kind of information a reasonable investor would take into consideration when deciding whether to buy or sell a security. Some examples of information about a company that may be material are:

- A proposed acquisition or sale of a business.
- A significant expansion or cutback of operations.
- A significant product development or important information about a product.
- Extraordinary management or business developments.
- Changes in strategic direction such as entering new markets.

Competing Fairly

We believe in free and open competition and never engage in practices that may limit competition or try to gain competitive advantages through unethical or illegal business practices.

Do not engage in conversations with competitors about competitively sensitive information or engage in any anti-competitive behavior, including setting prices or dividing up customers, clients, members, suppliers, or markets. Antitrust laws are complex and compliance requirements can vary depending on the circumstances, so seek help with any questions about what is appropriate and what isn't.

Be Alert to Anti-Competition Warning Signs

In general, the following activities are red flags, should be avoided, and, if detected, reported to the **Legal Department**:

- Sharing our Company's competitively sensitive information with a competitor.
- Sharing competitively sensitive information of business partners or other third parties with their competitors.
- Attempting to obtain nonpublic information about competitors from new hires or candidates for employment.

Watch Out For

— **Collusion**—when companies secretly communicate or agree on how they will compete. This could include agreements or exchanges of information on pricing, terms, wages, or allocations of markets.

— **Bid-rigging**—when competitors or service providers manipulate bidding so that fair competition is limited. This may include comparing bids, agreeing to refrain from bidding, or knowingly submitting noncompetitive bids.

— **Tying**—when a company with market power forces customers to agree to services or products that they do not want or need.

— **Predatory pricing**—when a company with market power sells a service below cost to eliminate or harm a competitor, with the intent to recover the loss of revenue later by raising prices after the competitor has been eliminated or harmed.

What If?

I received sensitive pricing information from one of our competitors. What should I do?

You should contact the Compliance Officer without delay and before any further action is taken. It is important, from the moment we receive such information, that we demonstrate respect for antitrust laws, and we make it clear that we expect others to do the same. This requires appropriate action that can only be decided on a case-by-case basis and may include sending a letter to the competitor.

Cooperating with Government Investigations and Audits

From time to time, workforce members may be asked to participate in internal and external investigations and audits that are conducted by our Company or by government officials. All workforce members are expected to fully cooperate with all such requests and ensure that any information provided is true, accurate, and complete.

If you learn of a potential government investigation or inquiry, immediately notify your manager and the Legal Department before taking or promising any action. If you are directed by our Company to respond to a government official's request, extend the same level of cooperation and again, ensure that the information you provide is true, accurate, and complete.

Watch Out For

— **Falsified information**. Never destroy, alter, or conceal any document in anticipation of or in response to a request for these documents.

— **Unlawful influence**. Never provide or attempt to influence others to provide incomplete, false, or misleading statements to a Company or government investigator.

Our Responsibility to the World

Corporate social responsibility is an integral part of our Company culture. We believe in making a positive difference in people's lives and engaging responsibly in charitable activities to make a positive impact in the communities where we live and work. As a Company, we contribute funds, time, and talent to support Company-wide programs and local causes. We encourage (but do not require) you to participate in the many initiatives we support.

We also encourage you to make a difference on a personal level, supporting charitable and civic causes that are important to you. Be sure your activities are lawful and consistent with our policies and that you're participating on your own time and at your own expense.

Watch Out For

- Putting pressure on colleagues to participate in personal charitable or volunteer activities.
- Using Company funds, assets, or the Judi Health names to further your personal volunteer activities unless you receive approval in advance.

Contributing Outside the Workplace

Everyone has the right to voluntarily participate in the political process, including making personal political contributions. However, as workforce members, we must always make it clear that our personal views and actions are not those of the Company.

Make it clear that your political views and activities are your own. You don't represent the Company.

Do the Right Thing

- Ensure that your personal political views and activities are not viewed as those of the Company.
- Do not use our resources or facilities to support your personal political activities.
- Follow all federal, state, local, and foreign election laws, rules, and regulations as they relate to Company contributions or expenditures.

Watch Out For

- **Lobbying**. Interactions with government officials or regulators that could be seen as lobbying must be discussed in advance and coordinated with the Legal Department.
- **Pressure**. Never apply direct or indirect pressure on another workforce member to contribute to, support, or oppose any political candidate or party.
- **Improper influence**. Avoid even the appearance of making political or charitable contributions in order to gain favor or in an attempt to exert improper influence.
- **Conflicts of interest**. Holding or campaigning for political office must not create, or appear to create, a conflict of interest with your duties at our Company.

What If?

I will be attending a fundraiser for a candidate running for local office. Is it okay to mention my position at the Company as long as I don't use any Company funds or resources?

No. It would be improper to associate our name in any way with your personal political activities.

I would like to invite an elected official to speak at an upcoming Company event. Would that be a problem?

You must get approval from the **Legal Department** *before inviting an elected official or other government official to attend a Company event. If the invitee is in the midst of a reelection campaign, the Company event could be viewed as an endorsement of the candidate. Depending on local laws, any food, drink, or transportation provided to the invitee could be considered a gift. In most cases, there would be limits and reporting obligations.*

Honoring Our Environment

We recognize our environmental and societal responsibilities. We are committed to sustainability and to minimizing damage to the environment as well as any potential harm to the health and safety of workforce members, customers, clients, members, and the public.

Protect workforce member safety and the environment. Read and understand all the information provided by our Company that is relevant to your job and operate in full compliance with environmental, health, and safety laws and regulations.

Do the Right Thing

- Fully cooperate with environmental, health, and safety training, and with our Company's periodic compliance reviews of our products and operations.
- Stop work and report any situation that you believe could result in an unsafe working condition or damage to the environment.
- Provide complete and accurate information in response to environmental, health, and safety laws, regulations, and permits.
- Be proactive and look for ways we can minimize waste, energy, and use of natural resources.
- Contact the **Legal Department** if you have any questions about compliance with environmental, health and safety laws, and policies.

Do you need additional guidance? We have a variety of resources to contact for help:

Issue or Concern	Contact
Ask questions, report potential misconduct, or other ethical concerns	Your manager or a member of senior management Human Resources Legal Department Compliance Department
For legal questions	Legal Department
To view Company policies	Policy Resources Hub
For media inquiries	Marketing
For information security	IT Security
For general security concerns	Human Resources
For general privacy concerns	Privacy Department

Anonymous Reporting Hotline
Compliance and Fraud, Waste, and Abuse (FWA)

Website: Mitratech

Toll-Free Telephone:

- USA & Canada (all languages): 855-222-0934
- Mexico (Spanish): 800-461-1552

Final Notes: Nothing in this Code of Conduct constitutes a contract of employment/contract with any individual or entity. Additionally, nothing in this Code of Conduct changes the at-will nature of employment/contract at the Company.

Oversight: The Board of Directors review and approve the Code of Conduct annually as part of their oversight responsibilities.

Code of Conduct last edited: October 7, 2026
Code of Conduct reflects update to company name effective July 15, 2026.