



Your world leading CDMO.

Code of Ethics and Business Conduct

Jeannie L. Metzinger

Jeannie L. Metzinger
SVP Chief Compliance &
Quality Officer
May 1, 2024



Welcome

to PCI Pharma Services

PCI is a trusted partner in the delivery of lifesaving medicines around the world and we are proud of our role in improving patient health. PCI has a strong Quality, Safety and Environment Social Governance (ESG) culture which impacts every business decision we make and is a top priority for all employees.

PCI is committed to fostering environmentally sustainable performance, honoring a diverse and inclusive culture, and creating positive impact on our employees, supply partners, customers, investors, patients, and the communities in which we live and work.

As a world class CDMO, we relentlessly strive to deliver better health outcomes for the patients we serve by combining our experience and expertise in science, manufacturing, and technology with our pristine customer service.

Our teams are committed to providing the highest level of Quality, exceptional customer service, maintaining a culture of engagement, and delivering the best solutions for our customers.

Teamwork and open communication are critically important to our working environment. PCI succeeds when we combine the best ideas of approximately 6,000 associates. Our culture of continuous improvement, embracing best practices, and discovering new ways of approaching daily challenges allow PCI to be a market leader.

We maintain our leadership position by building on this collective expertise. Our people make the difference.

I wish you all the best in your career at PCI and look forward to our shared success.

Sincerely,

A handwritten signature in black ink, appearing to read 'Salim Haffar', with a stylized flourish at the end.

Salim Haffar
CEO

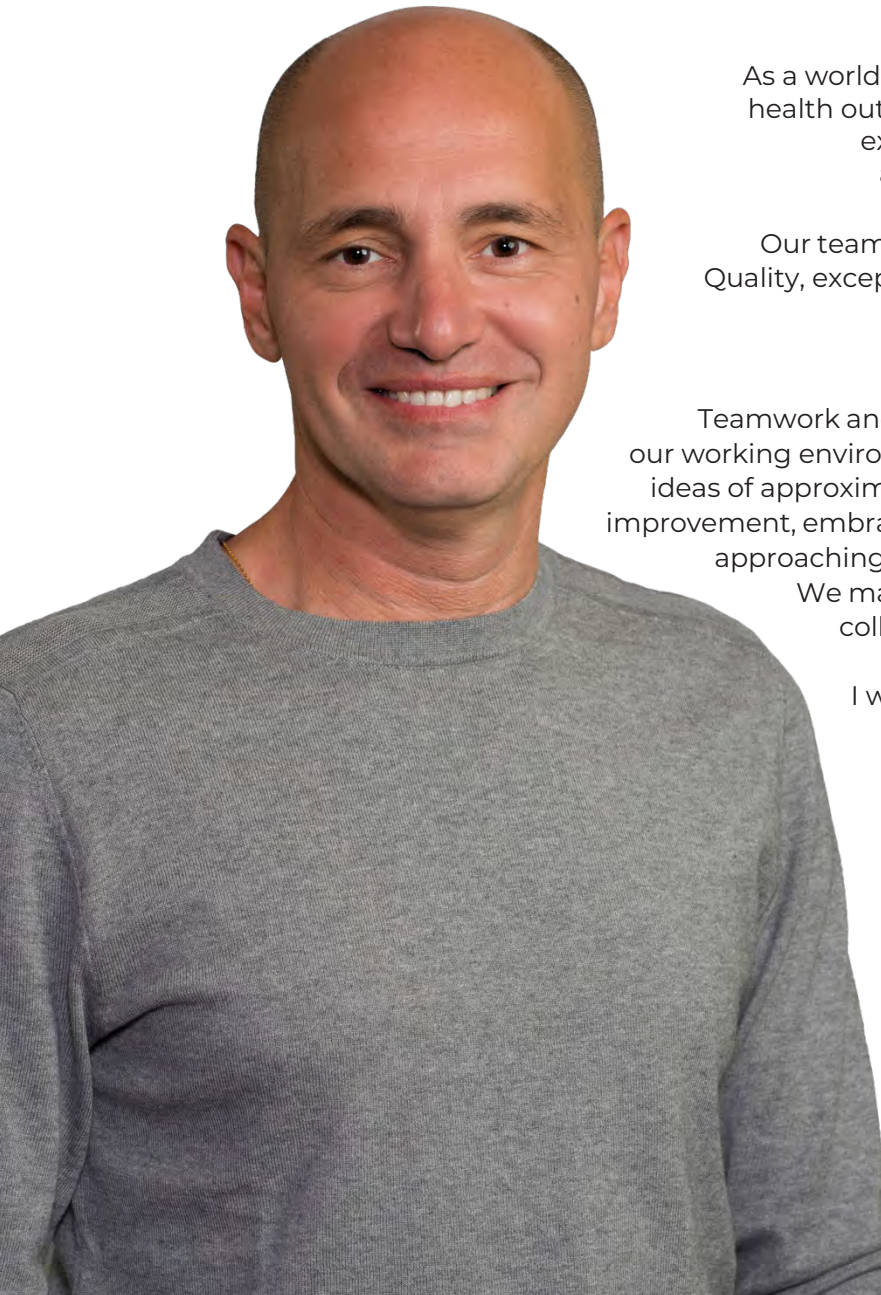


TABLE OF CONTENTS

INTRODUCTION	3
Reporting Violations	3
Anti-Retaliation Policy	4
PCI Ethics Hotline	4
Investigating and Responding to Reports	4
What Can You Expect When You Report a Suspected Violation of the Code?	5
Disciplinary Actions	5
WORK ENVIRONMENT	6
Honest and Ethical Conduct	6
Employee Responsibilities	6
Equal Employment Opportunity and No Harassment	6
Safety and Health	7
Human Rights Abuse	7
Animal Testing	7
Conflict Minerals	7
Political Activities	7
COMPLIANCE WITH LAWS AND THE CODE	8
Global Business	8
Compliance with Fraud and Abuse Laws	8
Personal Disclosure Requirements	8
Antitrust, Competition and Fair Dealing Laws	9
Anti-Bribery and Anti-Corruption	9
Drug Diversion	10
Public Communications and Filings	11
Government Audits and Investigations	11
FDA and Similar Drug Laws	11
Financial Reporting	11
Cooperating with Auditors	12
COMPANY PROPERTY, INFORMATION AND BUSINESS PRACTICES	13
Company Property	13
Confidential and Proprietary Information	13
Cybersecurity	13
Intellectual Property / Work Product	14
Use of Time, Equipment and Other Assets	14
Accuracy and Integrity of Business Records	15
Records and Information Management	15
Review of Contracts	15
Business Communications	15
Third Party Vendor and Supplier Engagements	15
Privacy of Personal and Third Party, Nonpublic Data	16
CONFLICT OF INTEREST	17
Other Conflicts	17
Improper Payments; Accepting or Giving Gifts	18
Meals and Entertainment	18
Seminars and Training Sessions	18
Loans	18
ADMINISTRATION OF THE CODE	19
Responsibility	19
Reporting of Code Decisions and Investigations	19
Chief Compliance Officer	19
Local Compliance Officer	19
Acknowledgment and Training	20
Waivers	20
Further Information	20

INTRODUCTION

The PCI Pharma Services (PCI) Code of Ethics and Business Conduct prescribes values and principles to which PCI is committed in order to guide our business practices around the globe. This Code specifies non-negotiable minimum standards of behavior in the workplace and while acting on behalf of our Company (even if outside the physical workplace) and while participating in Company-related social events. We expect our consultants, contractors, representatives and suppliers to be guided by these principles as well.

As a PCI employee, you are responsible for understanding and complying with the Code, Company policies and procedures and all applicable laws. The Code applies to all of our global business practices and in the event that legislation in a region where you carry out your duties differs from the language in this Code, the Code will be implemented in accordance with the relevant legislation.

The Code does not address all workplace conduct and/or all situations that may occur. The Company maintains additional policies and guidelines that may provide further guidance. There are also numerous resources available to assist you in performing your duties and responsibilities in compliance with law and company policy, including this Code and PCI training programs. You should seek guidance when in doubt about the proper course of action from your Local HR representative, Chief Compliance Officer (“CCO”) or Members of the Compliance Committee (see Administration of the Code page 19).

Reporting Violations of the Code

You have many different channels to report violations or potential violations of this Code, including your supervisor, manager, Human Resources, Chief Compliance Officer, members of the Compliance Committee or call the PCI Ethics Hotline (page 4).

If you have good faith reason to believe that a violation of the Code has occurred, or you are asked to violate the Code, don’t remain silent; report such violations or suspected violations, immediately. Depending on the circumstances, failure to report may itself violate the Code.

PCI will protect any employee who raises a concern in good faith, but it is a violation of the Code to make a false accusation knowing it is false, lie to investigators, or interfere or refuse to cooperate with a Code investigation. Honest reporting doesn’t mean you have to be right when you raise a concern; but you must believe in good faith that the information you are providing is accurate.

Employees are expected to cooperate fully and honestly in any investigations conducted by the Company of alleged violations of the Code. Failure to cooperate may be cause for disciplinary action up to and including termination of employment or the business relationship with the Company.

Any individual who knowingly and in bad faith provides false, incomplete or misleading information as part of an investigation (whether such individual is the complainant, the accused or a witness) will be subject to disciplinary action up to and including termination of employment or the business relationship with the Company.

Remember that no unethical or illegal acts can be justified by saying that they benefited the Company, or that they were directed by a higher authority in the organization. We all have an obligation to uphold the ethical standards of PCI.

Raising issues promptly allows the Company an opportunity to deal with the issue and correct it, ideally before it becomes a violation of law or a risk to the health, safety, or security of our employees or those who purchase or use our products, or to the reputation of our Company.

In addition to reporting alleged violations, you are encouraged to contact the Local HR representative, Chief Compliance Officer (“CCO”) or Members of the Compliance Committee (see Administration of the Code page 19), when faced with an ethical dilemma as it is always best to obtain guidance before acting.

Anti-Retaliation Policy

The Company will not engage in or tolerate any unlawful retaliation against a whistleblower or anyone who raises a concern or complaint in good faith under the Code (even if it turns out that the employee was mistaken) or serves as a witness or otherwise participates in an investigation as part of a complaint or concern raised under the Code. The Company also will not engage in or tolerate retaliation against someone associated with an individual who has raised a concern.

There is never a penalty for reporting a violation of the Code in good faith. People in positions of authority cannot stop you. Efforts to try and stop a report of an actual or suspected violation of the Code will lead to disciplinary action which may include termination of employment.

Insofar as possible, the confidentiality of the whistleblower will be maintained.

PCI has Open Door, Anti-Retaliation, Whistleblowing and Confidentiality policies to protect employees.

PCI Ethics Hotline

The employee that raised the concern may also report suspected violations by means of the compliance hotline which permits anonymous reporting. The Lighthouse Services, LLC PCI Ethics Hotline information is posted throughout our facilities. The hotline is intended to supplement, not replace, other channels for communicating questions and concerns within the organization. The Compliance Hotline is available by phone 24 hours a day, 7 days a week and is operated by specially trained third-party representatives. Callers are given a case number and have the opportunity to call back to check on the status of his/her report.

North America (US and Canada)– 1-800-603-2869

Outside of North America, please dial the phone numbers below to reach AT&T.

Australia– 1-800-551-155 / then dial 1-800-603-2869

Germany– 0-800-225-5288 / then dial 1 - 800-603-2869

Ireland–1-800-550-000 / then dial 1-800-603-2869

Spain– 900-99-0011 / then dial 1-800-603-2869

United Kingdom– 0-800-89-0011 / 800-603-2869

Investigating and Responding to Reports

The process for investigating an alleged violation of the Code is to gather and evaluate the information. If you are the subject of an investigation, the Company will give you the opportunity to respond except in special circumstances, such as when a government agency is directing a secret investigation.

We will make a determination whether the Code or the law has been violated and take appropriate corrective action if we conclude there has been illegal or improper conduct including, as appropriate, termination of the involved individual(s).

The Compliance Committee reviews founded violations and reports them to the Chief Executive Officer (“CEO”) and the Board of Directors (the “Board”). The Company is required by law to report all illegal acts to the appropriate government agency.

What Can You Expect When You Report a Suspected Violation of the Code?

- Your concerns will be treated promptly, seriously, and fairly and confidentially;
- You will be treated with dignity and respect;
- You need not identify yourself, although a more thorough investigation can be conducted if you are willing to share your identity;
- Your communication will be kept confidential as much as reasonably possible. PCI will make best efforts to protect your confidentiality; allegations will be disclosed only as necessary to investigate and/or take corrective action or as otherwise required by law;
- PCI will make good faith, reasonable efforts to resolve your concern promptly;
- PCI will make good faith, reasonable efforts to inform you of the outcome of the investigation including corrective action. In some circumstances it may be inappropriate or unlawful to inform you of the outcome, such as when a government authority requires confidentiality about the outcome;
- PCI will determine whether it will inform you of any discipline that may result from the investigation except as required under law; and
- The Company takes its obligations very seriously and will take the appropriate actions in response to violations of the Code, even if these actions are not visible to you.

Disciplinary Actions

The Company strives to impose corrective action (including discipline up to and including discharge) that fits the nature and circumstances of the Code violation.

Each situation will be evaluated and handled individually based on the nature, severity and frequency of the violation but could include reprimand, probation, suspension, reduction in salary, demotion or termination of employment.

In addition, corrective action (up to and including termination) will be taken against any employee who directs or approves the action that constitutes an infraction or who has knowledge of such actions and does not take prompt measures to report, prevent or correct them. Corrective action may include reporting to the appropriate governmental authorities. When the Company has suffered a loss due to a violation of law or this Code, it may pursue legal remedies against the individual(s) responsible.



WORK ENVIRONMENT

At PCI diversity, equity, and inclusion are at the core of our Company's purpose to serve as the bridge between life changing therapies and patients. We are committed to cultivating an inclusive workplace by holding ourselves accountable to the highest standards of understanding, fairness, respect, and equal opportunity at every level.

We envision a PCI community where everyone can belong and grow, and we strive to make this vision a reality by continuously and intentionally assessing our people practices, policies and programs, marketing approach, and workplace culture. Please refer to our ESG page on our company website to stay up to date with company objectives and initiatives relating to diversity, equity, and inclusion.

Honest and Ethical Conduct

PCI promotes high standards of integrity by conducting our business in an honest and ethical manner. We expect our employees to act with integrity and honesty in all workplace actions.

Employee Responsibilities

Each employee is expected to work in a cooperative manner with co-workers, management, supervisors, customers, and vendors. In addition, you must abide by the Code and all domestic and international laws, regulations, policies and guidelines in the workplace.

In addition to the responsibilities described above, supervisors must provide positive leadership and serve as a role model by not only complying with but also enforcing the Code.

Supervisors must fully support and comply with government regulations and Company policies and programs. They must take corrective action when necessary if an employee commits an offense in violation of those regulations, policies and/or programs.

Equal Employment Opportunity and No Harassment

PCI is committed to ensuring equal opportunity during employment, development and advancement without regard to any classification. All employment decisions, policies and practices are in accordance with the applicable federal, state and local anti-discrimination laws.

PCI will not engage in or tolerate unlawful discrimination (including any form of unlawful harassment or retaliation based on a person's sex, gender, pregnancy or childbirth, age, race, color, religion, creed, national origin, ancestry, ethnicity, citizenship, immigrant status, military status, veteran's status, mental or physical disability, medical condition, AIDS/HIV status, victim of domestic abuse, violence or stalking; genetic information, sexual orientation, gender identity or expression, marital status, familial status, partnership status or membership in any other protected group).

This entire Equal Employment Opportunity policy applies to all of the Company's officers, directors, managers, supervisors, employees and applicants.

The Company also will make reasonable accommodations for applicants and employees per PCI's policies, procedures and ESG initiatives (for example, measures for integration of senior employees and employees with disabilities, measures to promote wage equality and gender/minority inclusive environment).



Safety and Health

PCI is committed to providing a drug-free, safe, and healthy work environment, and to observe environmentally sound business practices. All employees are required to comply with environmental, health and safety laws and regulations as well as PCI safety and health rules and practices. In addition, you must report accidents, injuries and/or near misses immediately as well as any concerns about unsafe equipment, practices, or conditions.



Human Rights Abuse

PCI prohibits practices such as human trafficking, forced labor, physical abuse of workers, restricting workers' freedom of movement, confiscation of passports and worker documentation, failure to pay minimum or overtime wages where required by law, illegal child labor and any and all such human rights abuse.

Animal Testing

PCI does not perform animal testing at any of our facilities.

Conflict Minerals

As a socially responsible company, PCI supports the goal of the Dodd-Frank Wall Street Reform and Consumer Protection Act, Section 1502 of preventing armed groups in the Democratic Republic of the Congo and adjoining countries from benefitting from the sourcing of Conflict Minerals from that region. Such Conflict Minerals include tin, tungsten, tantalum, and gold. PCI is committed to working with suppliers to educate them on these matters; suppliers are expected to supply materials to PCI that are "DRC Conflict-Free".

Political Activities

PCI encourages individual participation in the political process. You must only participate on your own time and at your own expense in a manner consistent with relevant laws and Company guidelines. You must not give the impression that you are representing PCI and you may not use the Company's resources, including fax, phone or email, to personally engage in political activity.

COMPLIANCE WITH LAWS AND THE CODE

PCI is committed to conducting business in accordance with all applicable laws and regulations, as well as our own policies regarding ethical and compliance responsibilities. As such, all employees must comply with laws applicable to activities performed on behalf of PCI as well as Company policies. If a provision of the Code conflicts with the applicable law, the law controls.

Global Business

You are expected to comply with the Code and all applicable laws in the countries to which you travel, in which we operate and where we otherwise do business. These laws include those prohibiting bribery, corruption or the conduct of business with specified individuals, companies or countries.

Depending on your position, you may be subject to the laws, rules or regulations of many countries around the world. In the event, that local laws and regulatory requirements differ from those of the United States, the stricter set of laws and regulatory requirements generally applies, with limited exceptions. If such limited circumstances apply, you will be so informed.

In the event of a conflict between the Code and the law or regulation, the law or regulation shall control and must be applied. If you have questions about which laws, regulations, and policies apply to your work, contact your local HR representative, Chief Compliance Officer (“CCO”) or Members of the Compliance Committee (see Administration of the Code page 19).

Compliance with Fraud and Abuse Laws

You must never engage in fraudulent or any other dishonest conduct involving the property or assets or the financial reporting of the Company. Any substantiated acts of fraud and other dishonest conduct may not only entail disciplinary actions but also could result in criminal charges. Any suspected fraudulent or other dishonest activity must be reported immediately to the local HR representative, Chief Compliance Officer (“CCO”) or Members of the Compliance Committee (see Administration of the Code page 19).

Fraud can include, but is not limited to: forgery; misappropriation of Company assets; embezzlement; unauthorized handling or reporting of transactions; intentionally overcharging customers; and falsification of Company business records or financial statements; money laundering. Money laundering can be defined as transforming the proceeds of crime into the legitimate economy, and can often be seen in connection with other types of crime such as terrorism, trafficking, corruption and tax evasion.

PCI is firmly opposed to all forms of fraud and money laundering, and is committed to complying with all applicable anti-fraud and anti-money-laundering laws to conduct responsible business.

Personal Disclosure Requirements

If you have been excluded, debarred or suspended, or have become otherwise ineligible to participate in US federal healthcare or procurement or non-procurement programs, or if you are under investigation for certain civil or criminal offenses for which you may become

excluded, debarred or suspended, you must disclose this information immediately to Human Resources, Chief Compliance Officer (“CCO”) or Members of the Compliance Committee (see Administration of the Code page 19).

Antitrust, Competition and Fair Dealing Laws

PCI is prepared to compete successfully and will always do so in full compliance with applicable antitrust, competition and fair dealing laws. Agreements between competitors to fix prices, limit output, rig bids, or allocate customers, territories or lines of business are generally illegal, as are other types of conduct that harms competition.

Unfair or deceptive trade practices are also generally prohibited. These laws are complex and vary significantly from country to country. You must be aware of the laws in the country in which you operate.

If you are responsible for areas of the business where these laws apply you must:

- Avoid activities with representatives of other companies that may be viewed or construed as collusion or a violation of antitrust law;
- Not engage in communications with competitors on competitively sensitive topics or information;
- Understand that even joking about inappropriate topics, such as marketing or pricing strategies, could be misinterpreted so you should leave the conversation immediately;
- Avoid making false, misleading or disparaging statements about competitors;
- Not engage in unfair, deceptive or misleading practices;
- Always present Company services in an honest and forthright manner; and
- Not offer, promise or provide anything to a customer or supplier in exchange for an inappropriate advantage to the Company.

Anti-Bribery and Anti-Corruption

Anti-bribery laws forbid making, offering or promising anything of value to a government official to influence: a decision to award or retain business, the outcome of a government audit or inspection, or to influence tax or other legislation. Taken together, these laws are meant to ensure confidence in the integrity of the global business system.

As a U.S.-based company, PCI, its employees and its representatives are subject to the U.S. anti-bribery laws, and other international laws, some of which are described below, that are enforceable worldwide and cover all PCI operations, including all businesses, joint ventures, agents, and third-party representatives (such as independent contractors, general sales agents, customs brokers, consultants, finders, immigration agents, and tax agents, among others).

All PCI employees and representatives must comply with the laws below, regardless of the country in which you operate:

- **The Foreign Corrupt Practices Act (FCPA)** - The FCPA is a U.S. law which prohibits bribes to officials of non-U.S. governments and regulates US companies doing business abroad. The FCPA makes it illegal for employees and their agents or representatives of U.S. companies to give directly or indirectly anything of value to a non-U.S. government official, candidate for public office, political party or party official in order to gain an improper business advantage.
- **UK Anti-Bribery Act** - The UK Anti-Bribery Act is broader than the U.S. FCPA. It prohibits not only bribery of a government official, but also commercial bribery and receipt of bribes. Violations of this regulation include being bribed or bribing another person, the bribery of foreign public officials, and the failure of a commercial organization to prevent bribery on its behalf.



- **The Anti-Kickback Law** - As applicable, the U.S. Anti-Kickback Law prohibits offering anything to influence the recipient to purchase or recommend a healthcare product or service that is reimbursed by a federal healthcare program so that a healthcare provider's treatment recommendation is not influenced by motives of personal gain or enrichment and that the government does not pay for unnecessary or inappropriate products and services. Equivalent laws exist under state laws and around the world.

You should be aware that the offering or giving of improper benefits in order to influence the decision of the recipient, even if he or she is not a government official, may not only entail disciplinary actions but also result in civil and criminal charges, and exclusion, disbarment, or suspension from participation in a US federal health care program.

Further, the Company's policy is to select vendors, suppliers, consultants and contractors based on the merits of their products, services and business practices and to purchase supplies based on need, quality, service, price and other terms and conditions of sale.

Drug Diversion

Employees who illegally possess, sell, use, or divert controlled substances will have their employment terminated and their conduct may be reported to law enforcement agencies. They also subject themselves to state and federal prosecution.

Public Communications and Filings

PCI files reports and other documents to government agencies and regulatory authorities, inside and outside the U.S., on a routine basis as required under law. In addition, from time to time, the Company makes other public communications, such as issuing press releases.

All communications made to a government agency require the prior approval of the CEO except if such communication is part of your job description or you have been given explicit authority by the CEO, CCO or a member of Compliance Committee to do so. However, you do not need prior approval to report a suspected violation of law to a government agency and the Company will not retaliate against you for doing so.

Depending upon your position with the Company, you may be called upon to provide information to help assure that the Company's public reports and communications are complete, fair, accurate and understandable. You must cooperate fully with the Company's accounting and internal audit departments, as well as the Company's independent public accountants and counsel.

Individuals involved in the preparation of public reports and communications must take all necessary steps to comply with our disclosure controls and procedures, which are designed to support full, fair, accurate, timely and understandable disclosure in our public reports and communications. If you believe that questionable accounting or auditing conduct or practices have occurred or are occurring, you should notify the CFO or Members of Compliance Committee.

If you believe in good faith that any public disclosure may contain inaccurate information or if you become aware of any information that you believe in good faith should be disclosed to the public, it is your responsibility to bring this information to the attention of the highest ranking individual at your location and the Chief Compliance Officer ("CCO") or Members of the Compliance Committee.

Government Audits and Investigations

PCI will cooperate fully with all government authorities in connection with requests for information or facility visits. If you are contacted by a government authority with regard to a non-routine request for information or a facility visit, immediately notify the highest ranking individual at your location and the Chief Compliance Officer ("CCO") or Members of the Compliance Committee, as appropriate, unless you are contacted by the government and instructed not to discuss the investigation with anyone at the Company. If appropriate, legal counsel will be engaged to determine what information needs to be provided to the relevant government authority.

FDA and Similar Drug Laws

Careful attention to product quality has a direct and substantial effect on our Company's reputation and performance and allows us to exceed customers' expectations. The Company's operations are subject to extensive regulations by the Food and Drug Administration (FDA), the Medicines and Healthcare products Regulatory Agency (MHRA), the Drug Enforcement Agency (DEA), the National Health Surveillance Agency in Brazil (ANVISA) and other regulatory agencies inside and outside the U.S. Employees must follow all regulatory requirements.

Financial Reporting

PCI follows strict accounting principles and standards; reports financial information accurately and completely in accordance with these principles and standards; and has appropriate internal controls and procedures so that our accounting and financial reporting complies with the law.

It is important that all transactions are properly recorded, classified, and summarized in our financial statements, books and records in accordance with our policies, controls and procedures, as well as all generally accepted accounting principles, standards, laws, rules and regulations for accounting and financial reporting.

If you have responsibility for or any involvement in financial reporting or accounting, you must be familiar with and comply with the Company's disclosure controls and procedures and its internal control over financial reporting. If you are a senior leader or officer, it is your responsibility to put in place appropriate internal controls and procedures in your business area that are understood and followed.

You may not knowingly conceal or falsify information, misrepresent PCI's financial performance or otherwise intentionally compromise the integrity of the Company's reports, records, policies and procedures. For example, you may not:

- Report information or enter information in the Company's books, records or reports that fraudulently or intentionally hides, misrepresents or disguises the true nature of any financial or non-financial transaction or result;
- Establish any undisclosed or unrecorded fund, account, asset or liability for any improper purposes;
- Enter into any transaction or agreement that accelerates, postpones or otherwise manipulates the accurate and timely recording of revenues or expenses;
- Intentionally misclassify transactions as to accounts, business units or accounting periods; or
- Knowingly assist others in any of the above.



Cooperating with Auditors

Our auditors have a duty to review our records in a fair and accurate manner. You are expected to cooperate with independent and internal auditors in good faith and in accordance with law.

In addition, you must not fraudulently induce or influence, coerce, manipulate or mislead our independent or internal auditors regarding financial records, processes, controls or procedures or other matters relevant to their engagement.

You may not engage, directly or indirectly, any outside auditors to perform any audit, audit-related, tax or other services, including consulting, without written approval from the Chief Financial Officer (CFO) or Members of the Compliance Committee.

COMPANY PROPERTY, INFORMATION AND BUSINESS PRACTICES

Employees must safeguard and make only proper use of PCI's property. You must seek to protect Company property from loss, damage, misuse, theft, fraud, embezzlement and destruction.

These obligations cover both tangible and intangible assets, including, know-how, confidential or proprietary information and information systems. Company assets also include business records (regardless of the form retained), the telephone system, computers, electronic communications, wireless devices, written materials, money, product, components, scrap, supplies, copy machines, vehicles, Company trademarks, etc.

Company Property

The theft of Company property may result in termination of employment and criminal prosecution. PCI treats workplace theft of property belonging to employees and visitors the same way it treats the theft of Company assets. It is your responsibility to return all Company property when you leave employment. You are responsible to report any actual or suspected theft, damage or misuse of property to Human Resources, the CCO or Members of the Compliance Committee, as appropriate.

Confidential, Restricted, and Proprietary Information

Confidential, restricted, and proprietary information includes but is not limited to: trade secrets, business marketing and service plans, strategic documents, engineering and manufacturing ideas, records, financial information, information on those third parties that purchase or use PCI products, suppliers and other third parties, software and hardware systems and related documentation, and all other information not in the public domain that is proprietary to PCI. Such information also includes personally identifiable information of employees.

Unless required by law, authorized by management, or as specifically necessary to fulfill your job duties, you shall not disclose confidential or restricted information or allow such disclosure. Furthermore, you must use best efforts to avoid unintentional disclosure by applying special care when storing or transmitting confidential information. In addition, do not discuss confidential information with personal acquaintances or in public places where others may over hear.

After you are no longer employed by PCI, you must not disclose any confidential information for any reason, or allow such disclosure, unless required by law. This obligation continues beyond the termination of employment. Upon termination, you must immediately return all confidential information in your possession or control and you may not retain copies of such confidential information.

Cybersecurity

The protection of electronic confidential, restricted, and proprietary information is critical to PCI's operations and the interests of third parties in the confidentiality of their information.

The misuse of PCI electronic information includes, by way of example, sharing information with or permitting access to unauthorized third parties; accessing information that you are unauthorized to access; introducing malware or a cyber-virus, hacking or otherwise accessing or using such information for unauthorized or unlawful purposes, and may result in termination and criminal prosecution.

It is your responsibility to immediately report to the Cybersecurity Office, PCI Legal, your HR representative, the Chief Information Officer (CIO) or Members of the Compliance Committee any actual or suspected cyber-incident that could adversely impact PCI's operations or a third party, such as an email containing sensitive information from a suspicious source.

Intellectual Property / Work Product

All formulas, patterns, devices, secret inventions, processes, and compilations of information, records and specifications, regularly used in the operation of the Company, whether used or created by you alone or with others (collectively referred to as "Trade Secrets"), are the exclusive property of PCI. You agree to take any additional steps, or execute any documents, that might be required to perfect the Company's title in the Trade Secrets.



All inventions, discoveries, processes, methods, compositions, formulae, procedures, protocols, developments and improvements, techniques, results of experimentation and testing, information and data, whether patentable or not, which are not generally known, (i) embodying or produced through use of the Company's Trade Secrets and associated know-how, or (ii) embodying or produced through inventions conceived, discovered or reduced to practice, whether alone or with others, by the Company's employees or others acting on behalf of the Company or with the Company's facilities or equipment, (the "know-how"), are the exclusive property of the Company. You agree to take any additional steps, or execute any documents, that might be required to perfect the Company's title in the know-how.

All original works of authorship and copyrights created by you, alone or with others, within the scope of your employment ("Copyright Works"), shall be considered works made for hire, as defined by Title 17, United States Code, Section 101(2) and/or the Copyright, Designs and Patents Act 1988 in the UK or other applicable law. You agree to take any additional steps, or execute any documents, that might be required to perfect the Company's title in the Copyright Works.

Use of Time, Equipment and Other Assets

All employees are expected to protect PCI's assets and ensure their efficient use. You must not use Company time, computers or other equipment for personal activities that interfere with or prevent you from fulfilling your job responsibilities.

In addition, you may not use Company information systems to create, send or store harassing, discriminatory, retaliatory, defamatory, pornographic, obscene or other illegal or offensive messages or materials.

To support the use of the Company's information systems in a manner that is consistent with the Company's legitimate business interests, authorized representatives of the Company reserve the right to monitor the use of these systems.

As such, employees have no expectation of privacy when using the Company's communication systems in terms of messages or materials that they create, send, store or receive. Use of the PCI's information systems by employees signifies consent to the Company's monitoring messages or materials created, sent, stored or received on the Company's communication systems to the maximum extent permitted by law.

Accuracy and Integrity of Business Records

We are all responsible for maintaining accurate and complete business documentation for purposes of PCI's reputation and credibility, and to comply with Company's legal and regulatory obligations.

Business records include but are not limited to financial statements, quality records, time records, billing statements, invoices, expense reports, payroll records, benefits claim forms and resumes, etc. You must strive to be accurate and complete when preparing information for the Company, but honest mistakes may happen. Only intentional efforts to misrepresent or improperly record transactions, or otherwise to falsify a business record are Code violations.

Records and Information Management

PCI must maintain, store and destroy business records in compliance with applicable legal, regulatory, environmental, tax, and employment requirements. You may need to maintain records beyond the normal retention period in the case of actual or threatened litigation or government investigation. If you receive a "Legal Hold" from Company legal counsel, you must not alter or discard any relevant information. Failure to do so could subject you and the Company to serious legal risks.

Review of Contracts

All significant vendor contracts should be reviewed by the Procurement/Purchasing Department along with legal guidance before being signed. Legal review helps PCI avoid contracts that are inappropriate or unlawful; identify and minimize unfavorable contract provisions; and enter into contracts that are appropriate for the business circumstances. Legal review is also necessary to ensure that the contract is signed by a Company officer or employee with the proper level of authority.

Business Communications

Business communication may eventually become public through a variety of means, including government requests for information or litigation. Therefore, all communications, including email, must be composed in a professional manner which, if reviewed by a third party, would reflect favorably on the Company and the employee.

Do not make any communications that include harassing, discriminatory, defamatory, retaliatory, pornographic, obscene or other legal or offensive remarks or other offensive communications. Do not make legal conclusions in your communications.

Employees may not respond to media inquiries about the Company unless authorized by the Company to speak on behalf of the Company. If you are contacted by the media about PCI, report the contact to the appropriate person according to the local site policy or procedure without providing any information to the media.

Third Party Vendor and Supplier Engagements

Third party vendors, suppliers, contractors, and consultants must comply with all applicable federal, state and local laws, this Code and any other applicable policies.

The Company may be held liable for actions by a third-party agent acting on the Company's behalf. We expect that our vendors will take no action contrary to the principles of this Code.

Accordingly, the Code will be communicated to each supplier to obtain its commitment to comply with the Code and any other applicable policies, such as those concerning anti-bribery, as a condition of doing business with PCI.

Privacy of Personal and Third Party, Nonpublic Data

Employees who handle the personal data of others must protect the privacy of an employee's personal information. You must limit access to the information to those who have a legitimate business purpose for seeing the information and you must take care to prevent unauthorized disclosure. You must handle personal data responsibly and in compliance with all applicable privacy laws, regulations and policies, including the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and applicable state and foreign laws regarding privacy.

In addition, you must handle the nonpublic information of others responsibly and in accordance with our agreements with them. Nonpublic information of others includes notes, reports, conclusions and other materials prepared by an employee based on the nonpublic information of others.

You should not knowingly accept information offered by a third party, including a customer, supplier or business partner, that is represented as nonpublic, or that appears from the context or circumstances to be nonpublic, unless an appropriate nondisclosure agreement has been signed with the party offering the information. You should contact the VP and General Council or a Member of the Compliance Committee to coordinate the appropriate execution of nondisclosure agreements on behalf of the Company.

Even after a nondisclosure agreement is in place, you should accept only the information that is necessary or appropriate to accomplish the purpose of receiving it, such as a decision on whether to continue to negotiate a deal. If more detailed or extensive information is offered and it is not necessary or appropriate for your immediate purposes, it should be refused. If any such information is inadvertently received, it should be transferred to the VP and General Council or a Member of the Compliance Committee CCO for appropriate disposition.

Once the Company has received nonpublic information, you should use all reasonable efforts to:

- Abide by the terms of the relevant nondisclosure agreement, including any obligations with respect to the return or destruction of the nonpublic information;
- Limit the use of the nonpublic information to the purpose for which it was disclosed;
- Disseminate the nonpublic information only to those other Company employees, agents or contractors with a need to know the information to perform their jobs for the Company.

You may not unlawfully obtain or use the materials, products, intellectual property, proprietary or nonpublic information or other assets of anyone, including suppliers, customers, business partners and competitors. You may not coerce or improperly induce past or present employees of other companies to disclose proprietary or nonpublic information of their former or other employers.

CONFLICT OF INTEREST

Actual, potential or perceived conflicts of interest may occur whenever an employee is in a position to influence a decision that may result in a personal gain for the employee or an immediate family member as a result of the Company's business dealings. Avoid any relationship, influence, or activity that might impair, or even appear to impair, your ability to make objective and fair decisions when performing your job.

Here are some ways in which a conflict of interest could arise:

- You have a personal relationship with a customer or supplier. This does not mean that you can never have a personal relationship with a customer or supplier, but if you do you must keep in mind that relationship may be perceived as a conflict of interest if it could impair your ability to make objective and fair decisions when performing your job;
- You have a personal relationship with an employee with whom you have authority;
- You have a direct or indirect financial interest in a customer, supplier or competitor greater than 5%;
- You have a direct or indirect financial interest in a transaction between the Company and a third party, such as through a relative or significant other; and/or
- You obtain outside employment or a directorship with a competitor, customer, or supplier.

Other Conflicts

The following are examples of other conflicts of interest that are prohibited. If you or a family member or member of your household:

- Takes advantage of the Company's opportunities for personal profits;
- Receives fees, commissions, services, or other compensation from a Company supplier, competitor or customer;
- Receives personal benefits as a result of your position in the Company;
- Uses the Company's property, information or position for personal gain; and/or
- Are in competition with the Company as an employee, owner, contractor, etc.

Any opportunity that may result in an actual, potential or perceived conflict of interest should be fully disclosed to the VP and General Council or a Member of the Compliance Committee.

In some cases, potential and perceived conflicts can often be resolved in a simple and mutually acceptable way. The Code cannot address every potential conflict of interest, so use your conscience and common sense and/or seek guidance.

PCI has sole discretion to approve, conditionally approve or disapprove participation in such relationships by an employee. We encourage you to seek guidance if you have any questions as to whether an interest in a transaction is significant. If it is determined that the transaction is required to be reported by law, the transaction will be subject to review and approval by the Compliance Committee.

The Company may at any time rescind prior approvals to avoid a conflict of interest, or the appearance of a conflict of interest, for any reason deemed to be in the best interest of the Company.

Improper Payments; Accepting or Giving Gifts

You should not authorize, offer, promise or give, or solicit or accept any improper payment of money or other items of value intended to improperly influence, directly or indirectly, any business decision or that otherwise violate law or create the appearance of impropriety.

You and your immediate family members may not give or accept gifts, services, perks, entertainment, discounts, travel, loans or other items of more than modest value by local standards, to or from those who are doing or seeking business with the Company as it may appear to compromise your ability to make objective business decisions in the best interest of the Company.



In addition, items of modest value are permitted only if they are not given or received on a regular or frequent basis and are not solicited. In no event may you authorize, offer, promise or give, or solicit or accept any payments of money, gifts, or other items of value to any government official; however you may give a gift to a government official if you have a personal relationship and the gift relates to that personal relationship, but you must report the gift to the Compliance Committee. You should contact the CCO if you have any questions as to whether a payment is proper.

Meals and Entertainment

You may accept occasional meals and entertainment from customers and suppliers if the event is attended by the customer or supplier, and the costs involved are in line with local custom for business-related meals and entertainment. Meals and entertainment purchased for customers and suppliers must support the legitimate business interests of the Company and should be reasonable and appropriate. Be sensitive to our customers' and suppliers' own rules on receiving gifts, meals and entertainment. All Company funds expended for business amenities must be accurately recorded in the Company's books and records.

Seminars and Training Sessions

From time to time, the Company's vendors may invite employees to vendor-sponsored meals, trade shows, educational seminars or similar events. Prior to accepting any such invitation, you must obtain approval from your department leader.

Loans

Loans from the Company to directors and executive officers are prohibited except as permitted under law and approved in advance by the Board or its Audit Committee. Loans from the Company to other employees must comply with law and be approved in advance by the CFO or a Member of the Compliance Committee.



ADMINISTRATION OF THE CODE

The procedures for handling potential violations of the Code have been developed to support the consistency in the process across the organization. These guidelines may be varied as necessary to conform to local law and/or locations. The Code is reviewed every 2 years and updated with the intent that it will reflect the Company's business practices, procedures, and policies and comply with the special requirements of government sub-contracting.

Responsibility

The responsibility for administering the Code rests with the Compliance Committee, with oversight by the Chief Compliance Officer. The Compliance Committee is comprised of senior leaders representing corporate governance functions as well as operations. This includes: Tom De Weerd, CFO; Angi Calkins, CHRO; Wayne Hull, CIO, Jeannie Metzinger, CCO, Melissa Wojtylak, VP and General Council and Lisa Estes, Sr Executive Director, Human Resources.

Reporting of Code Decisions and Investigations

The Members of the Compliance Committee report all pending investigations and events at the Compliance Committee Meetings. The Compliance Committee events, investigations and decisions are discussed at the Executive Leadership Meetings (ELT) for awareness and reporting except when an issue concerns an ELT member, in which case the issue would be discussed with the CEO.

Chief Compliance Officer

The CCO authorized to oversee daily compliance with this Code is the Chief Quality and Compliance Officer, Jeannie Metzinger. The CCO reports to Salim Haffar, Chief Executive Officer (CEO) except when an issue concerns the CEO, in which case the CCO will report to the Board directly.

Local Compliance Officer

The Local Compliance Representative authorized to oversee daily compliance with this Code at the local level is the Site HR leader.

Acknowledgment and Training

You will be assigned training on the Code of Ethics and Business Conduct in the PCI Learning Management System (LMS) or you will receive a copy of the Code if you don't have access to the LMS. You will either sign an Acknowledgement Form or complete and electronically sign an Acknowledgement for the training in the system. These required acknowledgements mean that you agree to abide by the provisions of the Code for the duration of your employment and in some cases, after your employment. You will receive compliance training on the Code on a periodic basis and you will be required to make similar acknowledgements throughout your employment.

Failure to read and/or complete the training on the Code of Ethics and Business Conduct or sign the acknowledgement form does not excuse an employee from compliance with the Code.

Waivers

Any waivers of provisions of this Code for officers of the Company must be approved by the CEO or Members of the Compliance Committee.

Further Information

Please contact the CCO or a Member of the Compliance Committee if you have any questions about this Code or require further information.

The most current version of this document will be posted on the Company's intranet and within Compliance Wire.

