Lyric

Code of Conduct

July 2023

TABLE OF CONTENTS

Page

Lyric
Code of Conduct Policy
Policy Contact: For more information, or if you have any questions or concerns about this Policy, please contact the Compliance Office at compliance-ethics-privacy@lyrichealth.com.

A MESSAGE FROM OUR CEO

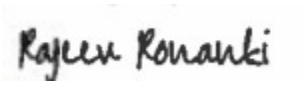
Character, commitment, community, courage, and customers – these are the very heart of our business. They are what fuel us, unite us, and drive us as pioneers in the ever-changing healthcare landscape. As we continue to build and refine these values as our foundation, honor, virtue, and integrity must be the pillars to keep us strong. And it's through our people how we will make this happen.

Here at Lyric, it is our duty to uphold a set of principles that keeps us morally and ethically sound. This Code of Conduct outlines the groundwork of who we are at Lyric and is meant to guide us in making the right decisions each day. It helps us take actions appropriately and with confidence while keeping our colleague's, partner's, and business' best interests in mind.

Our heritage continues through this code. It is expected and mandatory for all Lyric team members and external partners to ensure that the best practices set forth in the Code of Conduct are followed. You are also required to speak up when you see or suspect misconduct to The Ethics Hotline, by online or email. Lyric does not tolerate retaliation, and anyone who engages in retaliation will be subject to discipline. We respect the lives, wellbeing, and basic human rights of our employees, partners, and customers, and it is on us to maintain this simple idea in all we do.

Taking time to understand this code means you have a responsibility to yourself and others. I encourage you to review this document and understand how to apply these principles in the work you do each day. If you have any questions or need additional guidance, your manager will be able to point you down the right path.

Each of you holds the key to bringing our Code of Conduct to life. I value you for your loyalty, trust, and dedication to our business and thank you for committing to acting with purpose in all you do.



Raj Ronanki
Chief Executive Officer

POLICY CONTACT AND REPORTING CHANNELS

The Company is committed to upholding the highest standards of business conduct. We ask that you review the Code of Conduct and communicate any concerns about potential violations of this Code, other Company policies, or legal requirements to the resources set forth herein.

Reporting known or suspected violations, unethical behavior, or misconduct is everyone's responsibility.

Whether you:

- want to know about a compliance issue, the Company policies, or whether an activity is legal;
- see inappropriate behavior, a Code or policy violation, or illegal activity; or
- suspect inappropriate behavior, a Code or policy violation, or illegal activity,

you should reach out through the **Reporting Channels**. Don't wait for someone else to report. Looking the other way when it comes to unethical or unlawful conduct puts us all at risk.

To report a concern, violation, or suspected violation, or obtain more information about the Code, the Company policies, or legal requirements:

Compliance Hotline:
lyric.ethicspoint.com

Phone:
United States/Canada: 1-844-539-2320
Philippines: 1-800-1-322-0418

Compliance Office Email
The Compliance Office is available to answer questions, provide guidance or address your compliance, ethics, and business conduct concerns. You can contact the Compliance Office via email at compliance-ethics-privacy@lyrichealth.com. Note that Compliance Office members read all emails sent to this account, so it is not an anonymous way to communicate concerns.

ZERO TOLERANCE FOR RETALIATION POLICY

The Company has a zero tolerance policy for retaliation against anyone who, in good faith, raises a question, reports a concern regarding potential violations of this Code, other Company policies, legal requirements or other misconduct, or provides information or participates in an investigation regarding the same. Anyone who engages in retaliation is subject to disciplinary action, which may include termination of employment or no longer being able to provide services to the Company.

If someone has retaliated against you, report it immediately using any of the resources listed in the Reporting Channels section of this Code. If you see someone engaging in retaliation, you should also report it immediately.

CODE OF CONDUCT OVERVIEW

What does the Code of Conduct mean? While we work in the complex and ever-changing healthcare industry, our commitment to conducting business honestly, ethically, and in compliance with legal requirements remains constant. If the right course of action is not clear, use good judgment. Our success depends upon the decisions we make every day. All the Company team members are responsible for understanding the standards of business conduct embodied in the Code, the Company policies, and legal requirements that apply to their job. We are committed to incorporating honor, accountability, and trust in all we do to ensure we build confidence and assurance among our colleagues, our partners, and our business to make decisions that protect them each and every day.

We align our actions to the Code. The Code guides us to perform our daily work consistently with our values. We should all strive to make sound decisions and build and maintain trust with our colleagues and team members, customers, and business partners. We understand this trust is essential for the continued success of our business.

How does the Code work? The Code outlines the standards, values, and conduct that we expect all team members to adhere to in their daily work. The Code establishes basic standards of business conduct and provides information, tools, and other resources to help all team members make ethical decisions aligned to the values and goals of the Company. When making decisions, seeking guidance, or if you are unsure about what to do in a particular situation, you can first refer to the Code as a resource and guide.

The Code applies to all of us. The Code applies to everyone at every level of the Company. It applies to team members, officers, members of our Board of Directors, and any third parties who provide services at the direction of the Company, like agents, business partners, consultants, contractors, suppliers, or vendors. Third-party personnel can impact the Company's reputation through their behavior. For this reason, we seek agents, business partners, consultants, contractors, suppliers, and vendors who share our commitment to integrity, ethics, and compliance. If you are responsible for hiring or managing third-party personnel, it is your responsibility to ensure that they understand and comply with the Code, the Company policies, and all legal requirements. It is also your responsibility to hold third-party personnel accountable and monitor their activities. If you suspect that third-party personnel are in violation of the Code, the Company policies, or legal requirements, you must report the conduct.

We have shared responsibilities. Each of us is responsible for understanding and following the Code, the Company policies, and legal requirements. We also all share a responsibility to report any known or suspected violation of the Code, the Company policies, or legal requirements. If we fail to do so, the Company may be required to take disciplinary action, which may include termination of employment or no longer being able to provide services for the Company.

People leaders have special responsibilities. People leaders must set a good example for their team members, leading with integrity to model and inspire ethical conduct. Through everyday words and actions, people leaders should show they do business honestly by complying with the Code, the Company policies, and legal requirements. People leaders also must hold team members accountable when they violate the Code, the Company policies, or legal requirements. People leaders must:

- foster an inclusive environment;
- ensure team members have read and understand the Code and the Company policies and have taken all mandatory training courses;
- exercise appropriate supervision and oversight to ensure compliance with the Code and the Company policies;
- encourage team members to report known or suspected violations of the Code, the Company policies, or legal requirements, and ensure team members know where and how to report concerns;
- listen and respond to team members' concerns;
- immediately report and address suspected misconduct; and
- ensure team members are not retaliated against when they report.

Performance of these duties will be considered in all people leader evaluations.

Handling questions and concerns. We treat all concerns and complaints seriously, and will promptly, thoroughly, and fairly investigate all reports, taking appropriate action when necessary. We confidentially handle all reports, sharing information only on a "need to know" basis. We also protect our team members' identities to the extent possible when investigating reports of potential violations of the Code, the Company policies, or legal requirements.

Waivers. Waivers for any part of the Code must be approved by the Company Compliance Office. Waivers granted to members of our Board of Directors or executive officers must also be approved by the Company's Board of Directors or one of its committees. In the extremely rare situation that a waiver is approved, its scope will be limited as needed to protect the Company to the greatest extent possible. The Company will promptly disclose any such waivers for members of our Board of Directors and executive officers as required by law or regulation.

REPORTING OBLIGATIONS

Team members must report in good faith. It is our responsibility to ask questions and voice concerns when we encounter something that does not seem right. When we report concerns, unethical behavior or potential or suspected violations of the Code, we demonstrate our ability to incorporate honor, accountability, and trust in all we do, in line with the Company values.

How do I ask for guidance, voice a concern, or report an incident? In many cases, your people leader is in the best position to help you. However, if for any reason you are not comfortable talking about an issue with your people leader, you may contact the Compliance Office, HR, or the phone numbers in the Reporting Channels section of this Code. No matter whom you contact or what resource you choose, your concern will be promptly addressed and handled with the appropriate level of confidentiality. The Company has a zero tolerance policy for retaliation against anyone who raises a question or reports potential misconduct in good faith. Anyone who engages in retaliation is subject to disciplinary action, which may include termination of employment or no longer being able to provide services to the Company.

You Must Report:

- discrimination or harassment;
- privacy concerns;
- conflicts of interest;
- theft, fraud, or bribery;
- environmental or safety concerns;
- workplace violence, threats, or bullying;
- accounting or other financial issues;
- inappropriate gifts or entertainment;
- intimidation or retaliation;
- other threatening, concerning, or illegal behavior;
- code violations;
- policy violations; or
- legal requirement violations.

This is not a complete list of issues you should report. Anytime you see or suspect something is not right, you must report your concern.

The Company investigates compliance concerns. We promptly investigate all reports of conduct that may violate the Code, the Company policies, or legal requirements. All team members are expected to be truthful and fully cooperate with any investigation into an alleged violation of the Code, the Company policies, or legal requirements. Team members who fail to do so may be disciplined, possibly having their jobs terminated or no longer being able to provide services to the Company.

Communications with governmental entities. To facilitate appropriate investigation and resolution of compliance concerns, the Company requests that team members report compliance concerns first to the Company through the Reporting Channels section of this Code and allow the Company to fully investigate the concern. The Company's investigation will include an assessment of whether it is necessary to report the concern to governmental entities. Nevertheless, the Company team members may communicate, cooperate or file a complaint with any U.S. federal, state or local governmental or law enforcement entity concerning possible violations of any legal or regulatory requirement, and may make disclosures to any governmental entity that are protected under the whistleblower provisions of any law or regulation, so long as (1) such communications and disclosures are consistent with applicable law and (2) the information disclosed was not obtained through a communication that was subject to the attorney-client privilege (unless disclosure of that information would otherwise be permitted by an attorney pursuant to the applicable federal law, attorney conduct rules or otherwise). Any agreement inconsistent with the above language between the Company and a team member is deemed invalid and will not be enforced by the Company.

RESPECT IN THE WORKPLACE

The Company strives to create a supportive work environment where all team members can achieve their full potential and contribute to our values. The Company encourages collaboration and inclusion. Sharing, valuing, and supporting a wide range of ideas and viewpoints broadens our perspectives, inspires innovation and empowers us to achieve our goals.

We value diversity and promote inclusion. Our diverse workforce is one of the Company's many strengths, and we seek to enrich team members' work experience by providing challenging and meaningful opportunities. We provide equal employment opportunities and do not discriminate against anyone on the basis of race, color, ethnicity, religion, sex, pregnancy, childbirth, or related medical conditions, national origin, age, veteran status, disability, genetic information, marital status, sexual orientation, gender identify/expression, or any other characteristics protected by applicable legal requirements. If you believe you or others have been subjected to unlawful discrimination, you should contact your people leader, HR, the Compliance Office or any other resource identified in the Reporting Channels section of this Code.

We maintain a harassment-free work environment. The Company expects that all team members will treat each other with dignity and respect and promote a work environment where all team members can feel safe and comfortable. We do not tolerate verbal or physical conduct based upon a protected category that disrupts another's work performance or creates a hostile work environment. If you believe you or others have been subjected to unlawful harassment, you should contact your people leader, HR, the Compliance Office, or any other resource identified in the Reporting Channels section of this Code.

Individuals with disabilities. We provide reasonable accommodation to qualified individuals with disabilities to allow them to participate fully in our employment opportunities. If you believe you need an accommodation because of a disability, please discuss your request with your people leader, HR, the Compliance Office, or any other resource identified in the Reporting Channels section of this Code.

We respect human rights. The Company complies with all laws prohibiting human trafficking and maintains a zero tolerance policy against human trafficking that applies to all team members.

If you believe you or others have been subjected to human trafficking, or if you become aware of human trafficking, you should contact your people leader, HR, the Compliance Office, or any other resource identified in the Reporting Channels section of this Code.

RESTRICTED, CONFIDENTIAL, AND INTERNAL USE ONLY INFORMATION

We appreciate the trust our team members, customers, and other third parties place in the Company when they provide us with their Restricted, Confidential, and Internal Use Only information. We exercise care and discretion when handling such information.

We respect the privacy and security of Personal Information. Our customers, business partners, and team members trust us to respect and protect Personal Information and other sensitive information. **Personal Information** includes any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or

indirectly, with a particular individual, such as name, address, photo, birth date, phone number, social security number, or health, credit, or financial information. Personal Information is protected under various federal, state, and international privacy, security, healthcare, credit, and financial laws. We collect, store, access, use, share, transfer, and dispose of Personal Information responsibly. Given our role in the healthcare industry, we also receive, collect, maintain, use, or create a particular type of Personal Information, known as **Protected Health Information (PHI)**. We also respect and protect the sensitive nature of PHI and carefully maintain its confidentiality. See the **HIPAA Privacy Policies** for detailed guidance on handling and safeguarding PHI. All team members must follow the Company's privacy protection policies, which among other things require you to collect, access, use, share, transfer, and dispose of Personal Information and PHI only as necessary to do your job, to do so transparently, and to retain the information only so long as necessary for legitimate purposes, consistent with our records retention policies. Please review the **Records and Information Management Policy** for more details on handling and safeguarding the Company Information.

We protect confidential business information. All team members have an obligation to protect not only Personal Information, but also the Company Information that drives our business. We earn the trust of our team members and the companies with which we do business by following the Code, the Company policies and legal requirements. The Company Information may only be used for business purposes, not for personal use or gain. Before disclosing any Non-Public Company Information, there must be a legitimate business reason to do so. Non-Public Company Information may not be shared with anyone outside of the Company unless a non-disclosure or other appropriate confidentiality agreement is in place.

Help respect the privacy, security, confidentiality, and integrity of Personal Information and the Company Information:

- adhere to all the Company policies, procedures, rules, and guidelines addressed to privacy, confidentiality, record and information management, and information security;
- comply with applicable legal requirements;
- collect and use the minimum amount of information necessary to achieve legitimate business purposes;
- share information only with individuals who have a legitimate need for it and will protect it properly;
- follow the Company policies and guidelines for storing, handling, and destroying such information;
- immediately report any inappropriate disclosure or use of such information to the Company Ethics Hotline;
- new team members must protect the Non-Public Information of any former employers; and
- if a team member leaves the Company, the team member should return all Non-Public Information and may not share it with a new employer.

Maintaining Secure Information. Access to secure information is limited and depends upon a team member's job function. The Company regularly monitors its systems to be sure that information is accessed and used for appropriate, authorized activities, to discover any new

threats, and to look for ways to improve the security of its systems. We monitor and control all electronic and computing devices used to conduct the Company business or to interact with our internal networks and systems. As allowed by applicable legal requirements, the Company may inspect or monitor all messages, files, data, software, or other information stored on these devices or transmitted over our internal networks and systems to ensure compliance with the Company policies.

Incident Reporting. An incident is any situation where sensitive information may be lost, stolen, accessed, hacked, compromised, or improperly handled. An incident may involve Personal Information, PHI, or other Non-Public Company Information, or an attempt to gain unauthorized access to our systems or data. All team members must report any known or suspected incident involving the Company's or any of its team members' Non-Public Company Information or Non-Public Information belonging to a customer, business partner, contractor, consultant, supplier, or vendor through the Reporting Channels section of this Code.

CONFLICTS OF INTEREST

A conflict of interest exists when you have a personal, family, business, or other interest that could impair or appear to impair your ability to act in the best interest of the Company when making business decisions on behalf of the Company. Use your best judgment and avoid even the appearance of a conflict.

Disclose potential conflicts of interest. If a personal activity, investment, interest, or association could compromise – or even appear to compromise – your judgment, you must promptly disclose the conflict by contacting the Company Compliance Office. A conflict of interest often can be resolved in a simple and mutually acceptable way when discussed promptly and openly.

Is it a conflict? Ask yourself:

If I take this course of action:

- Will I feel obligated to someone else?
- Am I acting inconsistently with the core values of the Company?
- Is there a chance that my independent judgment could be compromised?
- Could it give the appearance of impropriety or divided loyalty?

If you answer "yes" to any of these questions, a real or perceived conflict of interest may exist. Disclose the potential conflict of interest by contacting the Compliance Office.

Common situations where conflicts of interest may arise:

Family and friends. Family and friends can create a conflict of interest if they work for the Company or one of our customers, business partners, contractors, consultants, suppliers, vendors, or competitors.

Financial interests. A conflict of interest can arise if you have a financial interest in a current or potential Company customer, business partner, contractor, consultant, supplier, vendor, or competitor.

Outside business activities. An outside business activity, such as a second job or working on a consulting basis, can create a conflict of interest if it competes with the Company or interferes with the work you do for the Company.

Hiring former government employees. Recruiting or hiring current or former government officials, whether appointed or elected, may raise conflict of interest concerns. You must not recruit or hire a current or former government official, whether appointed or elected, or government employee without obtaining prior approval from the their Manager, HR and Chief Compliance Officer. Refer to the Code section on doing business with the government for further guidance.

GIFTS AND ENTERTAINMENT

We recognize that the exchange of gifts or entertainment may help develop and strengthen our business relationships – but we do not give or receive gifts or entertainment that influence, or even appear to influence, business decisions. We give and receive gifts or entertainment in an ethical way that does not violate the Code, the Company policies, legal requirements, or third-party policies. All team members should study the **Meals, Gifts and Entertainment Policy** to learn the right way to give or receive an appropriate business courtesy. Whether giving or receiving a gift or entertainment, the **Meals, Gifts and Entertainment Policy** requires a team member to determine whether the courtesy is appropriate and lawful. This chapter describes the first steps you should take when considering giving or receiving a business courtesy, but you should always consult the **Meals, Gifts and Entertainment Policy.** All gifts and entertainment, whether given or received, must meet the Company's Criteria for Acceptable Business Courtesies.

Criteria for Acceptable Business Courtesies

- not solicited or requested;
- not perceived to improperly influence a business decision;
- not offered or received while a sales or procurement decision is pending;
- not conditioned on obtaining a sales or procurement decision;
- no personal benefit;
- infrequent;
- nominal value (not excessive or lavish);
- not cash or cash equivalent (no gift cards or gift certificates);
- occurs in an appropriate setting for business discussion;
- would not embarrass the Company; and
- is lawful under applicable laws.

USE OF THE COMPANY'S ASSETS

The Company assets are the tools and information we use in our work each day. We use these assets for legitimate business purposes and safeguard them from loss, theft, fraud, and misuse. The Company's assets are valuable and essential to operating the Company profitably and successfully.

We protect our physical assets. The tools we use to perform our work, including computers, telephones, and printers, are to be used for appropriate business purposes. Theft, carelessness, misuse, and waste of these assets have a direct impact on profitability. You may need to use the Company assets, such as computers, or the telephone, for occasional personal communications. With the exception of group collaboration software such as Microsoft Teams and WebEx, this use is permitted, as long as it is reasonable, meaning the use is minimal, does not interfere with your work performance or the work performance of others, and does not result in a significant cost or impact to our network. Group collaboration software may only be used for business purposes.

Appropriate use of information systems. All team members are required to use the Company's information systems in accordance with the **Records and Information Management Policy**. Your Company computer, network, and internet access must be used primarily for business. Occasional and reasonable personal use is allowed so long as it is minimal, does not interfere with your work performance or the work of others, and does not result in a significant cost or impact to our network. You should never use the Company's electronic systems for commercial or for-profit activity, or to:

- send chain letters or email spam;
- engage in illegal conduct;
- access or send sexually explicit, obscene, or offensive material;
- play games or gamble;
- create unapproved websites; or
- make personal video/conference calls.

Team members should have no expectation of privacy when using the Company's information systems. All activity conducted using these systems is and remains the property of the Company. The Company reserves the right at any time and for any reason to review and monitor the use of its information systems as permitted by legal requirements.

We safeguard our intellectual property. The Company's intellectual property is a valuable asset, and we invest heavily in its development. We protect our intellectual property by obtaining patent, trademark, copyright, or trade secret protection, and by taking steps to prevent inappropriate disclosure, use, or loss of such information. We vigorously enforce our rights to these assets. We also respect the intellectual property rights of others.

Electronic communications. When you send emails, voicemails, or access the internet at work, it is important to remember that your words and actions represent the Company. Team members should strive to use clear, accurate, respectful, and professional communication in all

of our business interactions, both within and outside the Company. Ambiguous and unprofessional communications, whether oral or written, can harm the Company.

Communicating with the public. We are committed to providing the public with relevant and appropriate information about the Company and communicating the information in a way reasonably designed to provide broad distribution of the information to the public. To maintain our reputation and ensure the public is consistently and accurately informed, only authorized individuals may communicate on behalf of the Company with the media. Press releases and all media and investor contacts are to be made only through a designated Company spokesperson. Unless you receive prior approval, you must decline the opportunity to respond to any inquiries for news or information about the Company. You must avoid creating any impression that you are speaking on behalf of the Company in any personal communications such as blogs, user forums, chat rooms, and bulletin boards.

Social media. We encourage communication and collaboration among team members, customers, business partners, contractors, consultants, suppliers, and vendors. However, the broad, instantaneous reach of social media significantly increases the importance of communicating responsibly, and managing private, sensitive, and confidential information in accordance with our policies and legal requirements. Ensure that you appropriately represent the Company's interests when making authorized Company communications and distinguish your personal opinions from those of the Company.

You also are expected to protect the Company's Non-Public Company Information and respect the privacy of team members, customers, business partners, contractors, consultants, suppliers, and vendors when using social media. If you have been entrusted with Restricted, Confidential, or Internal Use Only Information, you must not disclose it unless specifically authorized to do so. Do not publish maliciously false information that might embarrass or damage the reputation of another team member, customer, business partner, contractor, consultant, supplier, or vendor.

BUSINESS RECORDS

The Company maintains accurate business records. We are honest, accurate, complete, and timely in all aspects of our recordkeeping. Maintaining honest, accurate, complete, and timely records demonstrates integrity and builds trust in our stakeholders. Each of us has an obligation to follow all internal controls in recording and maintaining the Company's books and records. Accurate information is required to make good business decisions.

We are careful and accurate. We follow the Company's accounting controls to ensure our books, records, and accounts honestly, accurately, completely, and timely reflect all Company transactions, including how our funds and other assets are used. We never falsify or alter any financial record. We record all transactions properly and never delay or accelerate reporting of profits or expenses.

The accuracy of our books, records, and accounts also contributes to the quality of the financial and other information we provide to government agencies and make available to the public. We are committed to making full, fair, accurate, timely, and understandable disclosures.

We watch for unusual activity. We stay alert for irregularities or inaccuracies in our books, records, and accounts, and never give in to pressure from anyone to falsify a record or ignore something unethical. You must never knowingly engage in activities or conduct business with

individuals involved in money laundering – a process in which funds generated through criminal activity (such as terrorism, drug dealing and fraud) are moved through legitimate businesses to hide their criminal origin. Suspicious accounting practices could be a sign of fraud, bribery, or some other illegal act. Report such conduct immediately.

We manage and retain our records appropriately. The responsible creation, storage, maintenance, and disposal of records is important in helping us maintain financial integrity and meet our legal, tax, and regulatory requirements. You must retain the Company records as described in the **Records and Information Management Policy**. Records that have met their retention requirements should be properly destroyed. Do not dispose of any information that is subject to a legal hold. The records cannot be destroyed, altered, or deleted until you have been notified that the legal hold has been removed.

Adherence to Accounting and Financial Processes. Team members involved in any aspect of our accounting or other financial processes, must:

- follow all internal processes, controls, and accounting or other financial principles, ensuring that our records accurately and timely reflect all transactions;
- be honest, accurate, timely, and complete in all aspects of recordkeeping (including accounting records, financial statements, expense reports, time sheets, purchase orders, invoices, etc.);
- not establish any undisclosed or unrecorded funds, liabilities, or assets for any purpose;
- never falsify or mischaracterize any book, record, account, or transaction;
- not make any payment – regardless of form – on the Company's behalf without adequate supporting documentation and required approval; and
- apply payments received from customers properly.

Cooperation with audits. The Company and all team members are expected to cooperate with any audit. Such cooperation requires accuracy, candor, and responsiveness. You must never try to alter or destroy data, make any false, misleading, or inaccurate oral or written statement or influence, pressure, mislead, or manipulate any auditor in connection with any review of the Company's financial or other records.

FOLLOWING THE LAW

Our business partners and clients look to us for operational excellence. Because of this, we strive to perform our work in a transparent and ethical manner, and in compliance with legal requirements wherever we operate.

Anti-Kickback Statute (and similar state laws). In the United States, federal and state anti-kickback legal requirements prohibit the offering of, paying for, or requesting or receiving anything of value that is intended to influence the purchase of a healthcare product or service that may be reimbursed by any federal healthcare benefit program. Such programs include Medicare, Medicaid, and Tricare, any state healthcare benefit programs, and in some cases, a payer of healthcare products or services. Such offers or "kickbacks" may include any item of value, or compensation of any kind, such as money, commissions, credits, discounts, prebates, rebates, free products or services, or gifts or entertainment. These legal requirements are

drafted broadly and affect a variety of our business arrangements. Please review the **Anti-Kickback Policy** for more information.

False Claims Act (and similar state laws). The United States False Claims Act (and similar state laws) makes it a crime for any person or organization to knowingly make a false record or file a false or fictitious claim with the government for payment.

Stark Law (Physician Self-Referral Prohibition Statute). The Stark Law prohibits a physician in the United States from referring Medicare and Medicaid patients for certain designated health services to an entity with which the physician or a member of the physician's immediate family has a financial relationship. Providers of designated health services may not bill for services that result from a prohibited referral.

Exclusions and debarment. Under federal and state law, certain individuals and entities may be excluded, suspended, or debarred from participating in government healthcare and procurement programs. Companies may face fines and penalties for allowing such excluded individuals or entities to participate in these programs. Because the Company engages with many health insurance companies that administer government health insurance plans (such as Medicare and Medicaid managed care plans), the Company does not knowingly employ or do business with any individual or entity that: (1) is excluded, suspended, debarred, or declared ineligible from doing business with the government; (2) has been convicted of an offense related to government contracting or a government healthcare or procurement program; or (3) is identified on any government Exclusion List. In the event you become disqualified, suspended, debarred, or declared ineligible from doing business with the government at any time during your employment or assignment with the Company, you must immediately notify your people leader. The Company conducts checks of the following Exclusion Lists prior to hiring or assigning any individual or entity to perform work on behalf of the Company and on a periodic basis thereafter:

1. The General Services Administration's "Excluded Parties List System" and System for Award System (SAM)– a list of parties excluded from receiving federal contracts, certain subcontracts, and certain types of federal financial and non-financial assistance and benefits;[1]

2. The Office of Foreign Asset Control's "Specially Designated Nationals and Blocked Persons List" – a list of people and organizations with whom United States citizens and permanent residents are prohibited from doing business;[2]

3. The Office of the Inspector General's "List of Excluded Individuals and Entities" – a list of people and entities who are not eligible to participate in federally funded healthcare programs;[3] and

4. All available state Medicaid exclusion lists.

[1] Available at https://sam.gov/content/exclusions.
[2] Available at https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists.
[3] Available at https://oig.hhs.gov/exclusions/exclusions_list.asp.

If any team member or contractor is added to an Exclusion List, HR, the Compliance Office, and the Chief Compliance Office will coordinate on an appropriate response, which may include termination of the employment or contract of the affected individual or entity.

Antitrust and competition laws. The Company is committed to operational excellence and standing out in our industry through legal and ethical means. Therefore, you should:

- never make false, misleading, or disrespectful comments about our competitors or their products or services;
- only use legitimate means of obtaining competitive intelligence;
- respect the confidential information and intellectual property of our competitors and other third parties; and
- always comply with antitrust and competition laws.

Antitrust and competition laws encourage free and fair competition in the marketplace and protect the public from unfair business practices. Examples of prohibited anti-competitive business practices include:

- agreeing with a competitor to raise, fix, or hold a price at which goods or services will be offered (price fixing);
- agreeing with a competitor as to when, if, or at what price, each will submit a bid in a bidding process (bid rigging);
- agreeing with a competitor to divide markets or sell only to customers in certain geographic areas (market division); and
- exchanging price or other competitively sensitive information with competitors.

As a general rule, you always should limit your contact with competitors and avoid conversations about prices, customers, and suppliers. Antitrust laws are very complex, and the risks of noncompliance can be severe. If you have any questions or need further information, please contact the Compliance Office.

Communications laws. In the United States, various federal and state laws regulate when, how, and if the Company may contact others, including our customers. These legal requirements include:

- complying with “do not call” and “no texting” lists;
- restrictions on faxing;
- restrictions on robo calls; and
- restrictions on sending emails.

Before implementing any marketing or other product or services communications campaign, you must obtain advance approval of such campaign. Consult the **Telephone and Electronic Communications and Policy.**

If you become aware of a potential violation of any legal requirements, whether discussed in the Code or not, you must report it.

DOING BUSINESS WITH THE GOVERNMENT

There may be additional requirements or obligations to consider when doing business with the government. Doing business with the government requires us to follow rules beyond those applicable to our commercial customers or suppliers. Activities that may be appropriate in the commercial business environment may be improper when interacting with government customers. We never want to appear as if we are trying to bribe or to exercise improper influence on government customers. If your work involves a government customer, you are responsible for knowing and complying with the applicable legal requirements, including meeting all contractual obligations. A violation of such requirements can lead to serious financial and reputational harm and result in the Company being prohibited from doing business with government customers.

Government procurement integrity. The Company team members must not attempt to obtain the following information from any source:

- procurement-sensitive government information;
- confidential internal government information, such as pre-award, source selection information; and
- a competitor's bid or proposal information.

If such information is inadvertently communicated to you by a consultant, contractor, supplier, vendor, or a government employee, you should promptly contact the Compliance Office.

Organizational conflict of interest. You must ensure that when competing for or performing a government contract there is no actual or potential organizational conflict of interest that would provide the Company unequal access to Non-Public Information, provide an unfair advantage in a competitive procurement, or impair our objectivity in providing assistance or advice to or performing work for a government customer. You must promptly report all actual or potential organizational conflicts of interest to the Compliance Office.

Restrictions on employing current and former government personnel. Many governments regulate the employment activities of current and former government officials, whether elected or appointed, to restrict the Company from gaining an unfair competitive advantage by hiring a current or former government official or employee. You must obtain advance approval from the Compliance Office before discussing employment opportunities with any former or current government employee.

Anti-corruption laws. We do not tolerate bribery or any form of corruption. You must not offer anything of value to obtain favorable treatment from a respective customer. This is true even in countries where bribery is common and local legal and cultural standards allow it. The Company complies with all anti-bribery and corruption laws in the locations where it does business. The Company prohibits anyone from offering, soliciting, or accepting a bribe, whether dealing with government officials, political parties or representatives from commercial organizations. We expect this same standard of integrity from all our third parties, agents, and anyone else with

whom we work on the Company's behalf. Please review the **Anti-Corruption Policy** for more information.

If an applicable law conflicts with the Code, we follow the law; however, if a local business practice conflicts with the Code, we follow the Code. When in doubt, reach out to an appropriate resource for guidance.

POLITICAL CONTRIBUTIONS AND ACTIVITIES

Engagement in political activities must comply and be consistent with legal requirements. In the United States, federal, state, and local laws regulate our ability to make political contributions and to engage in political activities, including lobbying. Many countries outside the United States have similar laws. Accordingly, all political contributions to be made with the Company funds, and all lobbying activities on the Company's behalf, must be approved in advance by the Chief Compliance Officer and Chief Executive Officer. The Company team members may, in their individual capacities, make contributions directly to candidates and political parties of their choice. However, any individual contributions should not be attributed to the Company, and contributing team members are responsible for ensuring that their contributions comply with applicable legal requirements. Please review the **Political Contributions and Governmental Activities Policy** for more information.

INSIDER TRADING

Do not trade on insider information. United States securities laws prohibit buying and selling shares of stock or other securities on the basis of non-public material information. This is called "insider trading." If you have access to non-public material information about the Company or another company, regardless of the source, you are not permitted to use or share that information for your personal benefit. All Non-Public material information about us, our owners, our customers, business partners, contractors, consultants, suppliers or vendors should be considered confidential information. If a team member trades securities of these entities while having non-public material information, or if a team member shares non-public material information with others who trade, this may constitute insider trading. We are all responsible for reviewing, understanding, and complying with applicable securities laws and regulations.

DEFINITIONS

Anything of Value. Anything of value is broadly defined and may include cash, cash equivalents, gifts, meals, entertainment, recreation, charitable donations, loans, travel expenses (airfare, hosting, etc.), job placements, consulting contracts, operational support, educational support or other payments, or free or discounted items.

Bribery. Offering, promising, or giving anything of value to gain an improper advantage or favorable business decision.

Cash Equivalents. Loans, stock, stock options, bank checks, travelers' checks, check or cash cards, gift certificates, money orders, investments securities, or negotiable instruments.

Close relative. Includes spouse, significant other, child, parent, in-law, or other devoted family member.

Company Assets. Anything the Company uses to conduct business, including equipment, supplies, vehicles, furnishings, computer systems, software, phones, and other wired and wireless devices. Also includes information, trade secrets, personnel, our brand, and our reputation.

Company Information. Information or data collected, accessed, stored, transmitted, used, disclosed or disposed of in connection with the Company business or otherwise related to the Company, team members, customers, business partners, and any entity or third-party providing services at the direction of the Company. For clarity, the Company Information may include but is not limited to Confidential Information, Personal Information, Restricted Information, and Internal Use Only Information. The Company Information does not include Public Information.

Confidential Information. Information intended for limited business use that is exempt from public disclosure because, among other reasons, such disclosure could jeopardize the privacy or security of team members, clients, or partners, and possibly violate federal or state laws. Disclosure of Confidential Information could cause significant harm to the Company and is limited to authorized individuals.

Conflict of Interest. Situations in which a team member's personal considerations or interests have the potential to affect or could have the appearance of affecting, their judgment or objectivity in their work for the Company.

Family. Family includes spouse, children, siblings, parents, grandparents, grandchildren, aunts, uncles, nieces, nephews, cousins, step relationships, and in-laws.

Good Faith. Acting in "good faith" means making a genuine effort to provide honest, complete, and accurate information.

Government Officials. Employees or agents of any government anywhere in the world, even low-ranking employees or employees of government-owned, affiliated or controlled entities. The term also includes political parties and party officials, candidates for political office, and employees of public international organizations, such as the United Nations.

Harassment. Unwelcome words, actions or behaviors that denigrate, disrespect, or belittle an individual or create a hostile, offensive or intimidating work environment because of a protected category. Sometimes, a person's conduct may be considered harassment even if it was not intended to be offensive.

Human Trafficking. Human Trafficking includes, without limitation, recruiting, harboring, transporting, providing, or obtaining a person for labor or services through the use of force, coercion, fraud, or deception, the abuse of power or of a position of vulnerability, or the giving or receiving of payments or benefits to achieve the consent of a person having control over another person for the purpose of exploitation. Exploitation includes, without limitation, involuntary servitude, peonage, debt bondage or slavery, the removal of organs, and sex trafficking, or other forms of exploitation.

Intellectual Property. Knowledge, ideas, discoveries, formulas, inventions and other intangible assets that have commercial value and are protected under copyright, patent, service mark, and trademark laws. Additional examples of intellectual property include technical inventories,

brands and logos, software code, presentations, databases, customer lists, process documents, product designs, and roadmaps.

Internal Use Only Information. Information that may be shared among team members, but not with outside parties unless an authorized nondisclosure agreement (NDA) has been signed. Examples include weekly status reports, team member contact information, and software documentation.

Kickback. A form of corruption that involves two parties agreeing that a portion of the money paid, or due to be paid, will be given back to the purchasing party in exchange for making the deal.

Legal Hold. A legal hold suspends all document destruction procedures to preserve appropriate records under special circumstances, such as anticipated or actual litigation or government investigations. The Compliance Office identifies what types of records or documents are required to be placed under a legal hold.

Material Information. Information that an investor likely would consider important in deciding whether to buy, hold, or sell securities of a company.

Money Laundering. Making money derived from unlawful activities “clean” by making it appear the money came from legitimate sources or transactions.

Need to Know. Team members who have a “need to know” information require access to that information (often confidential in nature) to do their jobs. If you are in doubt about whether a particular individual within the Company has a “need to know,” please contact HR or the Compliance Office.

Non-Public Company Information. Information about a business organization that is not generally available to or known by the public (also called “inside information”).

Personal Information. Information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual such as one of our employees or a website user or a household. Examples include name, address, birth date, phone number, or social security number.

Protected Health Information. Protected Health Information (PHI) is any individually identifiable health information, that (1) is created or received by a healthcare provider health plan, or healthcare clearinghouse; and (2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present or future payment for the provision of healthcare to an individual; and (3) directly or indirectly identifies the individual.

Restricted Information. Information intended for a limited group of individuals specified by name. Inappropriate disclosure of such information could result in serious detriment to the Company. Examples include merger and acquisition information, financial forecasts or results not yet public, and strategic planning information not yet public.

Retaliation. Taking adverse action against a team member in response to that team member's good faith report of an actual or suspected violation of the Code, the Company policies, or legal requirements.

Social Media. Online communication channels that provide an opportunity for content sharing, individual input of information, and interaction. Includes websites, chat rooms, blogs, news feeds, social networking sites, and special applications dedicated to posting and sharing comments, articles, opinions, ideas, information, and images.

ANNUAL CODE OF CONDUCT TRAINING

Each year the Company and all team members will engage in a Code of Conduct training. This training discusses the goals and objectives of the Code of Conduct, the Company policies and legal requirements. Specific topics include, but are not limited to, the following:

- the Company's values and commitment to incorporating honesty, accountability and trust in all we do, including acting in an ethical manner and in compliance with applicable laws;
- overview of pertinent laws applicable to the Company's businesses, including the federal anti-kickback statute, the False Claims Act, the Foreign Corrupt Practices Act, securities laws, antitrust laws, and privacy and security laws;
- the requirement that team members report potential noncompliance or violations of the Code or the Company policies;
- process and lines of communication for asking compliance questions or reporting potential noncompliance (including anonymous reporting when supported by the Company in the near future);
- prohibition against intimidation or retaliation for good faith reporting of potential noncompliance;
- privacy and security awareness;
- general compliance and fraud, waste, and abuse (FWA) training and any other compliance or FWA training as may be required by the published Medicare Compliance Program Requirements; and
- attestation that the team member is aware of, and will abide by, the Code of Conduct.

Completion requirements. Team members receive compliance training both as part of their initial orientation (within 90 days of initial hire or engagement) and annually thereafter. Successful completion of compliance training both during initial orientation and annually is a condition of continued employment or engagement.

Next Review Date: No later than December 6, 2023.

Version Table:

Version	Date	Description
Version #1	**12/06/2022**	**First CXT Portfolio Code of Conduct**
Version #2	**7/1/2023**	**Second Lyric Code of Conduct**