



Vendor Code of Conduct

Navitus Health Solutions, Epiphany Rx, and Lumicera Health Solutions (collectively “Navitus”) is committed to compliance with all applicable laws, regulations and contract requirements. In addition, we hold ourselves to the highest ethical standards on behalf of our clients and members. To help ensure we maintain our compliance and ethical standards, we work closely with our vendors and business partners.

Our vendors are business partners who are important to our success and play a critical role in servicing our members and clients, whether directly or indirectly. This Vendor Code of Conduct (Code) is provided to you as an easy way to communicate our expectations as your company fulfills the terms of the contract. This Code is a guide and does not include all possible activities. Please share with your employees and contact us if you have a question about an activity not included in this Code.

Compliance Obligations

Vendors are expected to have mechanisms to enable employees, including temporary employees, or affiliates of vendor to report non-compliance, violations of this code of conduct, or other grievances. Such methods should protect the individual reporter from retaliation and offer anonymity. Navitus has several methods for reporting including via confidential, toll-free hotline, email, or mail. All good-faith reporting is protected under the Navitus Non-Retaliation Policy. Vendor may distribute the Navitus toll free Compliance Hotline number which is **1-855-673-6503**.

Vendor is expected to take all reasonable actions to address non-compliance and remediate, mitigate, and engage in corrective action to comply with laws and regulations, comply with [Guiding Principles on Business and Human Rights](#), health and safety protections, labor laws, and environmental protections. Navitus reserves the right to audit Vendor where performance of services is dependent on such compliance.

Gifts and Business Gratuities

Navitus discourages you from providing any gifts, meals, entertainment or other business gratuities to Navitus employees, consultants or pharmacists. While we appreciate the occasional pen with your business name, items such as the following are not appropriate:

- Gifts or entertainment of any kind to any Navitus staff during the selection, negotiation or purchasing stages of a contractual arrangement.
- Gifts or entertainment that could be perceived as a bribe, payoff or advantage.
- Cash or cash-equivalents, such as checks, gift certificates/cards or stock.
- Gifts or entertainment that violate the law.

Conflicts of Interest

Conflicts of interest between a vendor and Navitus staff (or the appearance of a conflict) should be avoided. When an actual, potential or perceived conflict of interest occurs, that conflict must be disclosed, in writing to Navitus.

- While Navitus employees may occasionally have secondary employment, no Navitus employee member may work for a vendor that has a contractual relationship with Navitus.
- No Navitus employee may participate on the board of a vendor with whom Navitus does business.
- Navitus will not engage with an individual who has been employed by Navitus within the last 24 months and who has been assigned as Navitus' representative by the Vendor for products, sales, negotiation, contracting, promotion or other activities where the former employee's confidential and proprietary knowledge about Navitus is a component of that assignment.

Compliance with Laws

Vendors are expected to conduct their business activities in compliance with all applicable laws and regulations, including Medicare and Medicaid. Vendors are also expected to take appropriate action against any of its employees or subcontractors that have violated such laws.

Privacy and Security

State and Federal privacy laws, such as the requirements of the Health Insurance Portability and Accountability Act (HIPAA) require Navitus and its Vendors to maintain the privacy and security of patient information (PHI). If a vendor has access to Navitus PHI, the vendor is responsible for ensuring that all employees who provide services to Navitus are trained on HIPAA Privacy and Security Rules and is expected to provide an annual attestation that such training has been completed. In addition, if vendor uses or discloses PHI on behalf of Navitus, the vendor will be expected to enter into a Business Associate Agreement.

Employed or Contracted Persons

Navitus will not knowingly do business with any vendor if it is, or any of its officers, directors or employees are excluded, debarred or ineligible to participate in any Federal or State health care program. To ensure no exclusion exists, Navitus vendors must screen all employees (including temporary and contracted), officers and directors against Federal exclusion lists before hire or engagement and on monthly thereafter. These lists are the U.S. Department of Health and Human Services, Office of Inspector General List of Excluded Individuals and Entities (LEIE) and the General Services Administration's System for Awards Management (SAM). Vendors may be expected to provide an annual attestation that such exclusion screening has occurred.

Navitus will not knowingly do business with any vendor engaged in corruption, illegal sourcing or anti-boycott activity or involved in human trafficking, slavery, or child labor. Navitus expects a vendor to implement and enforce systems and controls to ensure that such abuses do not occur

in staffing, in operations, in supply chains, with downstream entities or in relation to services to Navitus. This includes but is not limited prohibiting any requirement for employees, temporary workers, or contractors to pay fees or expenses to secure work with Vendor and prohibiting the retention of identity documents as a condition of working for Vendor.

Fraud, Waste and Abuse (FWA)

Vendors are expected to report any suspected or actual acts of FWA regardless of the source or possible participants. Navitus will investigate allegations of FWA and, where appropriate, will take corrective action, including civil or criminal action.

Vendor Compliance Training

Navitus requires all vendors, including vendor employees, to participate in and complete general compliance and FWA training. The vendor must document and provide an annual attestation that training has been completed. Training can be completed using the CMS free training modules located on the CMS MLN website. In addition to compliance and FWA training, Vendors and their employees who qualify as Business Associates must also complete annual privacy and security training. This training can be completed using the vendor's training or by requesting a copy of the Navitus privacy and security training.

Vendor is obligated to comply with any additional regulatory or industry training requirements and maintain such evidence of training as needed by Navitus to represent the quality, knowledge, and/or regulatory awareness of the Vendor and its employees or contractors.

Business Record Retention

Navitus requires vendors to retain records related to services provided to Navitus for ten (10) years. These records must be made available to Navitus or a government auditor in accordance with applicable laws, regulations and contract terms.

Visiting Navitus

It is expected that any vendor who visits our campus additionally adheres to the Visitor Code of Conduct.

Environment and Sustainability

We are committed to protecting the environment. We expect our vendor to share our commitment and integrate proactive practices to minimize their environmental impact and waste, consider the full lifecycle of products or services, actively manage risks across their operations, products and supply chain and work for continuous improvement. We expect our vendors to partner with us to be good stewards of the environment by operating in a manner that actively manages risk, conserves natural resources and protects the environment. We expect our vendors to establish and apply a systematic approach to managing environmental issues, including potential risk from regulatory noncompliance, reputational loss and

opportunities for business growth through operational and product stewardship as applicable to the service rendered on our behalf.

Artificial Intelligence

At Navitus are committed to the ethical use of artificial intelligence in healthcare. We expect our vendors to notify us of the use of AI technologies in their products/solutions so that we can approve in advance and ascertain the impact and ethical implications of the AI use to our clients/members. In addition, we expect our Vendors to adhere to the following core principles* when developing or using artificial intelligence solutions on our behalf:

- **Engagement:** understanding, expressing, and prioritizing the needs, preferences, goals of people and the related implication throughout the AI life cycle.
- **Safety:** Attendance to and continuous vigilance for potentially harmful consequences from the application of AI in health and medicine for individuals and population groups.
- **Effectiveness:** Application proven to achieve the intended improvement in personal health and the human condition, in the context of established ethical principles.
- **Equitability:** Application accompanied by proof of appropriate steps to ensure fair and unbiased development and access to AI-associated benefits and risk mitigation measures.
- **Efficiency:** Development and use of AI associated with reduced costs for health gained, in addition to a reduction, or at least neutral state, of adverse impacts on the natural environment.
- **Accessibility:** Ensuring that seamless stakeholder access and engagement is a core feature of each phase of the AI life cycle and governance
- **Transparency:** Provision of open, accessible, and understandable information on component AI elements, performance, and their associated outcomes.
- **Accountability:** Identifiable and measurable actions taken in the development and use of AI, with clear documentation of benefits, and clear accountability for potentially adverse consequences.
- **Security:** Validated procedures to ensure privacy and security, as health data sources are better positioned as a fully protected core utility for the common good, including use of AI for continuous learning and improvement.
- **Adaptivity:** Assurance that the accountability framework will deliver ongoing information on the results of AI application, for use as required for continuous learning and improvement in health, health care, biomedical science, and, ultimately, the human condition.

*= From [Artificial Intelligence in Health, Health Care, and Biomedical Science: An AI Code of Conduct Principles and Commitments Discussion Draft - National Academy of Medicine](#), April 8th 2024

Employee Working Environment

We require that our vendors:

- Provide a working environment that meets or exceeds prevailing industry standards and local, regional, and national safety, occupational health and fire safety regulations.
- Provide adequate risk assessment, emergency plans, emergency equipment, and emergency trainings to ensure the safety of the work environment.
- Provide regular health and safety training to workers.
- Encourage workers to openly raise health and safety concerns and provide safeguards against retaliation.
- Provide required rest breaks to prevent excessive physical and mental fatigue.

In addition, Navitus expects its suppliers to maintain a health and safety management system to limit worker exposure to hazards and promote continuous improvement of working conditions and occupational health and safety.

Compliance with US Sanctions

As a condition of doing with Navitus, all vendors, contractors, etc. must comply with applicable US trade, export, and economic sanctions laws and regulations, including those administered by the US Dept of Treasury's OFAC.

Vendors shall not:

- Source, purchase, or distribute products or services that originate from, or are routed through countries, organizations, or individuals, subject to US government trade embargoes or sanctions
- Facilitate or engage in financial transactions on behalf of Navitus that involve sanctioned entities, banks, or jurisdictions.
- Utilize any subcontractor or affiliate that is owned or controlled by a sanctioned party or located in a restricted country.

Vendors are expected to maintain internal controls to ensure that their operations, financial practices, and supply chains remain compliant with all applicable sanction laws. Vendors must immediately notify Navitus of any known or suspected violation of these requirements.