PREMIER

2022

ANNUAL COMPLIANCE REPORT

CONTENT

Key Highlights
For The Year

Alan C. Sauber, Chief Ethics & Compliance Officer

This year's accomplishments demonstrate the ongoing collaboration between business leaders and the Corporate Compliance department in a combined effort to achieve Premier's growth goals. The team works diligently to keep the company in compliance with ethical standards, regulatory requirements and certification needs of the business. Some of the major accomplishments for the year include:

• Named one of the World's Most Ethical Companies by Ethisphere® Institute for the fifteenth consecutive year.

• Secured 100% completion of employee annual education and policy attestations for the all four quarters of 2022.

• Led the Privacy team with a seamless transition of the new Chief Privacy Officer starting April 2022 and added a new Compliance Specialist in July 2022.

• Successfully completed a KPMG Data Governance Audit with no high or medium risk findings.

• In addition to updating Premier's cookie functionality on its websites, the Privacy team established multiple internal and external policies and procedures to ensure compliance with California and other new state privacy laws. The team also completed a thorough review and update of Premier's public-facing Privacy Notice to reflect Premier's current processes and comply with applicable privacy laws.

• Partnered closely with Contigo Health leadership to identify gaps, provide education, improve communication, update policies and procedures, and ensure compliance with applicable privacy laws and regulations as this business segment expands its operations.

• Initiated and implemented a program and process that integrates Operational, Risk Management and Compliance functions for Clinical Intelligence, Applied Sciences, Remitra, Contigo Health and Conductiv operational planning and execution. This program seeks to proactively manage risks that involve more regulated solutions.

• Organized extensive support of new business activity for Contigo's Catavert product. Worked with internal teams to support legacy and prospective compliance obligations such as Utilization Review Accreditation Commission (URAC) and National Committee for Quality Assurance (NCQA).

• Created a new module within the Enterprise Governance, Risk and Compliance (GRC) platform to centralize System Security Plans (SSP). SSPs are a key tool in monitoring and managing Premier's information risks as they contain detailed system data points and metrics.

Leading With Integrity

Corporate Compliance Program

Premier's Board of Directors and executive leadership team play a critical role in promoting and maintaining a culture of integrity. Premier's Corporate Governance Guidelines and policies ensure that we operate in accordance with applicable laws and regulations for a publicly traded company including the security of proprietary, sensitive and protected health information as well as compliance with insider trading restrictions and other securities laws.

Our program aligns with the Federal Sentencing Guidelines, ensures that policies and internal controls are user friendly, and meets emerging compliance and ethics standards.
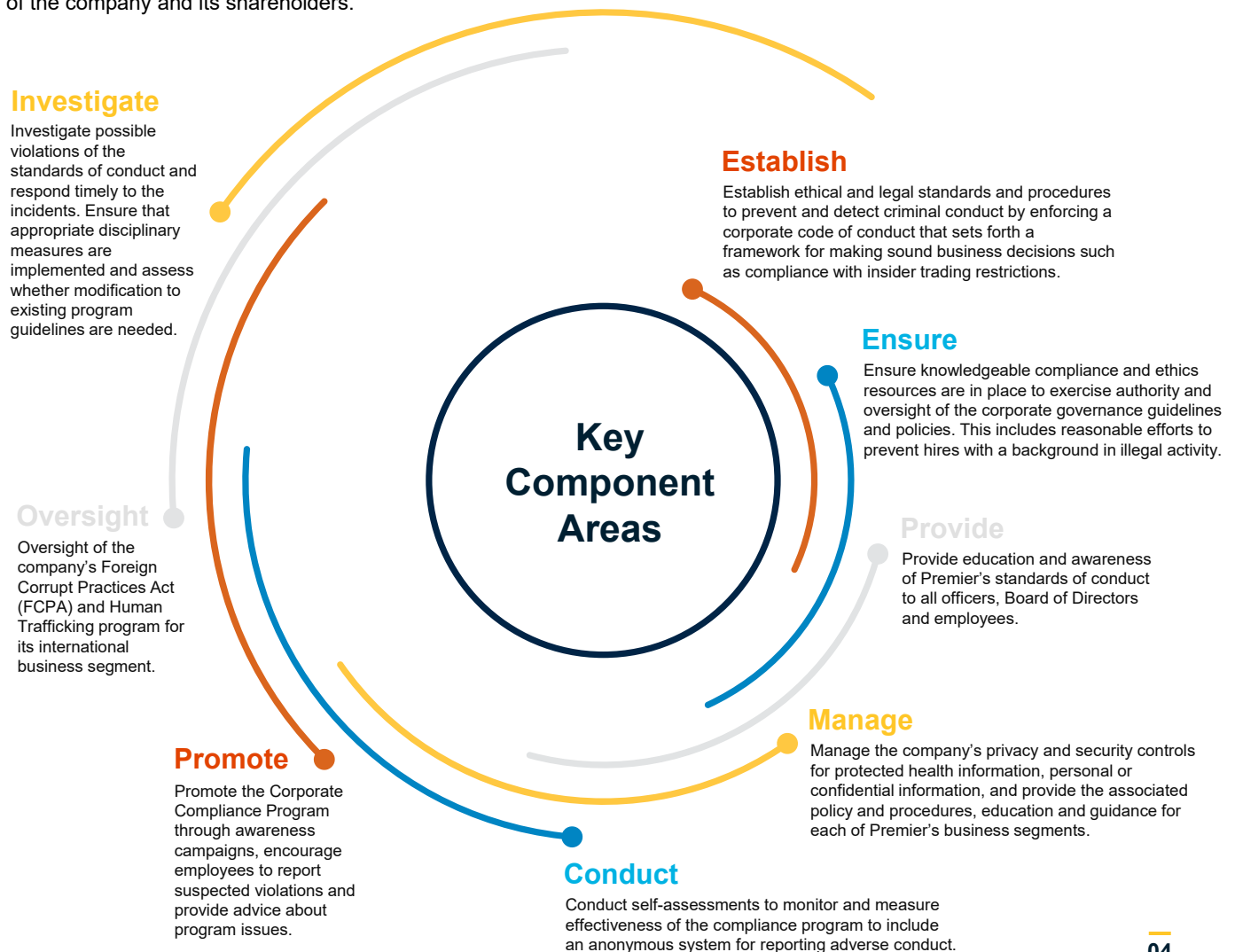
Board of Directors

The Corporate Governance Guidelines assist Premier's Board of Directors in the exercise of its duties and responsibilities and to serve in the best interest of the company and its shareholders.

Company

For employees, Premier's Code of Conduct sets the standards of business conduct at Premier. Our Code describes compliance expectations, assists in identifying unethical conduct, provides guidance to employees involving compliance matters, and explains investigations and resolution measures. It also enforces the company's zero tolerance for retaliation when reporting misconduct.

Business Rules

Premier maintains internal business rules for such topics as Administrative Fees, Custom Contracting and other programs that present greater risk to the organization. These rules define how we operate the programs and are verified at least annually for compliance.

Investigate

Investigate possible violations of the standards of conduct and respond timely to the incidents. Ensure that appropriate disciplinary measures are implemented and assess whether modification to existing program guidelines are needed.

Establish

Establish ethical and legal standards and procedures to prevent and detect criminal conduct by enforcing a corporate code of conduct that sets forth a framework for making sound business decisions such as compliance with insider trading restrictions.

Ensure

Ensure knowledgeable compliance and ethics resources are in place to exercise authority and oversight of the corporate governance guidelines and policies. This includes reasonable efforts to prevent hires with a background in illegal activity.

Oversight

Oversight of the company's Foreign Corrupt Practices Act (FCPA) and Human Trafficking program for its international business segment.

Provide

Provide education and awareness of Premier's standards of conduct to all officers, Board of Directors and employees.

Key Component Areas

Promote

Promote the Corporate Compliance Program through awareness campaigns, encourage employees to report suspected violations and provide advice about program issues.

Manage

Manage the company's privacy and security controls for protected health information, personal or confidential information, and provide the associated policy and procedures, education and guidance for each of Premier's business segments.

Conduct

Conduct self-assessments to monitor and measure effectiveness of the compliance program to include an anonymous system for reporting adverse conduct.

Conflicts of Interest

Premier's comprehensive policies and procedures are designed to ensure that employees, Board members, and non-employee committee and subcommittee members adhere to strict conflict of interest disclosure, divestiture and/or recusal requirements.

Board of Directors

Board members annually disclose potential conflicts that they and/or their immediate family member or related party may have. Conflicts may include affiliation with or managerial, consulting or employment relationships, personal, equity or other financial interests, compensation relationships with any company, vendor or firm and use of non-public information, Premier property and assets. **In 2022, 100 percent of all directors disclosed and resolved their conflicts of interest in accordance with company policy.**

Employees

Premier's Group Purchasing Code states that no employee of Premier or any Premier entity should own equity in any participating vendor. Upon hire, an employee is educated on both The Value of Integrity | Code of Conduct and Group Purchasing Code of Conduct. Employees complete a conflict of interest questionnaire upon hire and annually thereafter. If an employee owns an equity holding that is not permitted, he/she must disclose the conflict and then follow the Corporate Compliance department's prescribed steps to resolve it. Company-wide annual conflict of interest questionnaires launched October 12, 2022. **In 2022, 99.8 percent of active employees completed this questionnaire. The remaining 0.2 percent will be completed by January 31, 2023. Resolution of potential conflicts are underway and will be completed by mid-February.**

Member Committees

Sourcing committee and advisory subcommittee members disclose any potential conflicts annually and before all meetings or discussions. Premier's policy does not allow sourcing committee or advisory subcommittee members and/or their immediate family members to have extensive equity in a participating vendor. **In 2022, 100 percent of all committee and subcommittee members disclosed and resolved their conflicts of interest in accordance with company policy.**

Industry Involvement

Recognition

For the fifteenth consecutive year, Premier was named by the Ethisphere® Institute as one of the World's Most Ethical Companies. We were selected for this honor from among tens of thousands of companies around the world. A global leader in defining and advancing the standards of ethical business practices, the Ethisphere® Institute recognized Premier for continuing to raise the bar on ethical leadership and corporate behavior. Premier was the only company in the business services industry recognized this year.

Promotion

The Healthcare Group Purchasing Industry Initiative (HGPII), a voluntary association dedicated to ethical conduct and business practices, and to serve the confidence of the public and government officials, consists of ten GPOs who each commit to having its business practices be transparent to its customers, vendors and to the public and answer a comprehensive annual questionnaire known as the Public Accountability Questionnaire. This questionnaire requires detailed responses about ethics, compliance and contracting procedures.

On an annual basis, HGPII holds a Best Practices Forum for member GPO executives to share ideas, and work to improve ethics and compliance programs with their stakeholders. Forum participants include federal policymakers, ethics experts and a cross-section of healthcare supply chain vendors who gain knowledge about ways GPOs can improve communication with regulators and increase transparency to stakeholders and the general public. David Hargraves, Senior Vice President Supply Chain, is the current chair. This position helps Premier further advance our best practices within our supply chain segment of the business.
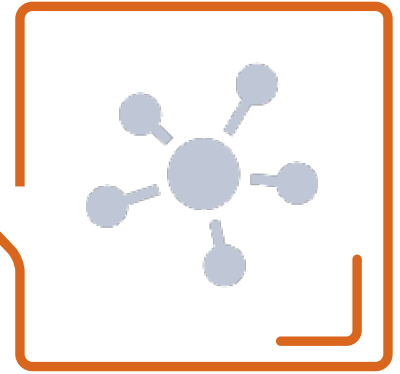
Affiliation

To foster and promote industry-wide adoption of compliance best practices, Premier Corporate Compliance staff participate and are members of the following professional organizations: Society of Corporate Compliance and Ethics (SCCE); Ethisphere® Institute Business Ethics Leadership Alliance (BELA); Healthcare Group Purchasing Industry Initiative (HGPII); International Business Ethics Institute; International Association of Privacy Professionals (IAPP), Information Systems Audit and Control Association (ISACA).

Premier's Chief Ethics & Compliance Officer participates in ongoing benchmarking, industry networking initiatives and speaking engagements including the Steering Committee and Working Group of the Healthcare Group Purchasing Industry Initiative (HGPII).

Privacy and IT Risk Management

New Privacy Developments

- The California Privacy Rights Act (CPRA) went into effect on January 1, 2023 and becomes fully enforceable on July 1, 2023. California Consumer Protection Act (CPRA) works as an addendum to the CCPA by strengthening rights of California residents (including eliminating the previous exclusion of HR data and B2B data under CCPA), tightening business regulations on the use of personal information (PI), and establishing a new government agency for state-wide data privacy enforcement called the California Privacy Protection Agency (CPPA). The first-ever CCPA enforcement action (a $1.2 million settlement with the retailer Sephora) was brought by California's Attorney General in August of 2022.
- The United States privacy legislative landscape has been active and privacy advocates are preparing for multiple data privacy laws to take effect in 2023. In addition to CPRA, the Virginia Consumer Data Protection Act, Colorado Privacy Act, Connecticut Data Privacy Act and Utah Consumer Privacy Act are all set to take effect in 2023. In addition, 2022 had 60 comprehensive consumer privacy bills considered across 29 states, with 5 states (Georgia, Indiana, Maine, Michigan and Vermont) considering comprehensive consumer privacy bills for the first time; this is a 106% increase from 2021 to 2022.
- Major changes were proposed to the federal "Substance Use Disorder" records confidentiality law (known as "Part 2") by the Department of Health and Human Services (HHS), which would better align Part 2 with HIPAA.
- In May 2022, a bipartisan group of legislators introduced the American Data Privacy and Protection Act (ADPPA) which includes federal preemption of state laws with some exceptions. This represents the first time federal data privacy legislation in the United States has progressed to a full chamber vote. As for its scope, it covers both for-profit businesses and non-profit organizations (which are currently exempt from most state privacy laws). It distinguishes between and imposes different obligations on "covered entities" that determine the purposes and means of data collection and "service providers" that process data at the direction of covered entities. Given multiple challenges with the current draft, it is likely that the ADPPA will continue to be debated in the incoming 118th Congress.
- According to the Office of Civil Rights (OCR), data breaches of medical entities have steadily increased over the past several years. Of the 10 largest health breaches in 2022, half involved "business associates" of medical providers. The likely reason business associate data breaches have increased is because bad actors know that one successful business associate attack may yield PHI from hundreds of covered entities.

Privacy Actions and Milestones

- External Privacy Policy and Premier website cookie functionality have been updated to comply with CPRA/CCPA notice requirements and opt-out rights.
- Internal HR Privacy Policy and data subject request procedures have been drafted in close collaboration with Premier's labor attorney, to ensure compliance with the rights of California employees and contract workforce. Implementation is scheduled for early in 2023.
- Updated Premier's Information Security Agreement and contract templates terms for vendor/subcontractor engagements to require their compliance with new privacy laws. Premier continues to thoroughly vet third-party vendors/subcontractors through the Premier Impact Assessment process and require adherence to stringent cybersecurity standards.
- Expanded education of Premier's employees and contract workforce on their obligations regarding the use and protection of protected health information, personal information and confidential information, and reviewed/updated Premier policies and procedures to ensure workforce compliance with applicable privacy laws such as CCPA and CPRA.
- Premier's Privacy team continues to stay informed on state and federal privacy law changes, analyze their applicability to Premier and make updates as needed.

Alongside technology innovations and the frequent electronic exchange of health information, cybersecurity for medical devices and equipment has become a top priority for healthcare providers. Life sustaining medical devices, such as ventilators and infusion pumps, are now connected wirelessly to a variety of systems, networks and other tools within a hospital – ultimately contributing to the Internet of Medical Things (IoMT) and presenting potential points of breach as well as incremental costs and operating risk to providers.

Ongoing Cybersecurity Risk

Patient care disruptions and safety issues related to medical device security vulnerabilities are a critical concern as the number of IoMT medical devices is expected to skyrocket from 10 billion to 50 billion over the next decade. These cyberattacks not only threaten patient privacy and clinical safety and outcomes, but also a hospital's financial resources. According to a recent report[1], the average breach costs in healthcare surpassed $10 million in 2022, with the industry maintaining its top rank for costliest industry breaches for the 12th consecutive year. Alongside direct costs related to a breach, providers may see added costs in hardware, software, firmware and labor.

Cybersecurity risk management for medical devices is a shared responsibility among manufacturers and healthcare providers to address patient safety risks and ensure proper device performance.

Several factors have introduced ambiguities regarding accountability, including misaligned expectations on cybersecurity controls throughout a device's lifecycle, often ill-defined by the manufacturer. A lack of clear manufacturer-defined guidance on security requirements for devices, both new and old, is particularly problematic for providers when considering the comparative accountability for risk associated with non-compliance. For its part, the U.S. Food and Drug Administration (FDA) has released market guidance[2] for manufacturers on securing systems for medical devices, but confusion remains as to whether the guidance is binding because it remains in draft format.

One way to reduce ambiguity is to include specific cybersecurity verbiage in contracts. This helps to mitigate risk and keeps device manufacturers accountable for their role in the security management process. Premier, working with the University of Pittsburgh Medical Center (UPMC), has led this effort to develop baseline cybersecurity control expectations that manufacturers must formally attest to as conditions of sale/usage. This approach also requires manufacturers to provide a pre-distribution device designed with the goals of:

• Reducing cybersecurity intrusion and misuse;
• Improving availability, reliability and accuracy;
• Adhering to generally accepted security procedures over the anticipated lifespan of the device or equipment; and
• Proactively providing a Software Bill of Materials (SBOM) for all firmware and software associated with the use of the device or equipment.

Upfront collaboration and alignment between manufacturers and health systems during the sourcing process provides much needed clarity for both parties on agreed upon objectives and control assurances. Device manufacturers, for instance, can affect and improve the protection of systems, data and patient safety by incorporating technical safeguards during the product design phase – and by performing risk assessments and threat models for each use case involving IoMT medical devices to help identify potential safety risks.

New Federal Legislation to Enhance Security Protections

The Protecting and Transforming Cyber Health Care (PATCH) Act, part of the recent Appropriations bill signed into law in late December, gives the FDA greater oversight of medical device cybersecurity requirements by holding manufacturers accountable for developing products with appropriate security controls. The bill requires manufacturers to design, develop, and maintain processes and procedures to provide updates and patches throughout the lifecycle of their devices. The bill also includes key provisions on monitoring and identifying post-market vulnerabilities, developing a plan for coordinated vulnerability disclosure and providing an accounting of all software contained in a device.

Regulatory and Compliance Milestones

• Full-year SOC 2 (Systems Organization Controls) Type 2 report for Clinical Intelligence, Cost Management and Clinical Decision Support product lines, performed for the period of January 1 through December 31, 2022, is coming to a conclusion. Type 2 designates that there is a test of effectiveness to ensure our internal controls over the security, availability and confidentiality of our systems perform as designed.
• A SOC 1, Type 2 report for Premier's General Controls over Information Technology (GITC) and Contigo Health's Claims Processing Operations System. The SOC2 is more technology focused, whereas the SOC1 focuses on both technology and financial reporting controls.
• A Federal Information Security Management Act (FISMA) audit was performed on the Premier network, ecosystem and software solution suite. Written attestation resulting from this audit (Security Assessment Report (SAR) and Security Compliance Letter of Attestation (LOA)), not only serve as evidence of Premier's security hygiene, but also as official attestation from a reputable, licensed third-party that a comprehensive assessment was performed based on criteria relative to Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB), Security of Federal Automated Information Resources, National Institute of Standards and Technology (NIST), a Guide for the Security Certification and Accreditation of Federal Information Systems and "Security and Privacy Controls for Federal Information Systems and Organizations", and NIST Special Publication 800-53.
• Achieved 2022 Office of the National Coordinator for Health Information Technology (ONC-HIT) certification for Premier's TheraDoc and electronic Clinical Quality Measures (eCQM) Calculator, covering 2015 Care Cures Act requirements enabling customers to collect interoperability incentives from CMS.

Education and Reporting

Education

Below is a summary of the compliance educational programming completed in 2022.

Board Governance

Board members completed an online course that reviewed the Board Code of Ethics, Insider Trading Policy, Conflict of Interest Policy, Compliance Policy, Anti-Bribery Policy and Human Trafficking Policy. In addition, this course provided an overview of governance, risk and compliance. **In 2022, 100 percent of the Board of Directors completed governance education.**

Employee Compliance

As part of Premier's annual compliance education, employees completed an interactive course that provided an overview of our Code of Conduct. It explained why we have a Code and employee responsibilities related to our Code. The course reviewed the following compliance topics: ethical workplace conduct, records retention and social media. **In 2022, 100 percent of active employees completed this coursework.**

Anti-Corruption/ Human Trafficking

Premier continued to engage the International Business Ethics Institute to develop and deliver the annual education to review Premier's Anti-Corruption and Human Trafficking policies and increase knowledge of when and where to seek advice. **In 2022, 100 percent of S2S Global employees completed this education.**

Member Committee Compliance

All sourcing committee and advisory subcommittee members received education this year on Premier's Group Purchasing Code of Conduct, Confidentiality Policy, Conflict of Interest Policy and Insider Trading Policy. **In 2022, 100 percent of committee and subcommittee members completed this education.**

Compliance Educational Programming

Medicare Parts C and D Fraud, Waste and Abuse (FWA) and General Compliance

All new employees and select staff who are more likely to access protected health information (PHI) completed education courses on Medicare Parts C and D FWA and general compliance programs to satisfy the Medicare Parts C and D plan sponsors annual general compliance education requirements per the Code of Federal Regulations (CFR) and sub-regulatory guidance. **In 2022, 100 percent of new employees and select staff completed this education.**

Health Insurance Portability and Accountability Act (HIPAA)

Workforce members completed company-wide HIPAA awareness education on how to properly obtain, use, share, maintain and transfer protected data. **In 2022, 100 percent of employees completed this education.**

Group Purchasing

Administrative Fees

Our administrative fees are standardized for each competitive bidding process and stated in advance to all bidders in a category unless economic conditions require a different structure in the best interest of members. Our group purchasing agreements do not impose up-front administrative fees from participating vendors and prohibit administrative fees in the form of vendor equity.

During calendar year 2022, 16.6% of Premier contracts had administrative fees above 3% compared to 12.5% in 2021. All fees are disclosed and reported per Federal Regulatory Safe Harbor provisions.

Vendor Rights and Responsibilities

Our success is firmly rooted in developing mutually beneficial relationships with our vendors. Premier's Supplier Guide outlines these expectations including a statement of vendor rights and responsibilities and is publicly available on Premier's website. Premier takes vendor grievances seriously and offers several ways to resolve possible issues. Premier has its own vendor grievance process to ensure a vendor's ability to access Premier's contracting staff and leadership to address concerns or complaints relating to the contracting award process or decisions. A vendor may also submit an inquiry related to the contracting process or award decisions. In most instances, this latter process is sufficient to address a vendor's concerns.

Disclosure of Vendor Payments

Consistent with Medicare safe harbor rules pertaining to the reporting of GPO administrative fees, Premier annually discloses to its members the amount of administrative fees received with respect to purchases made by or on behalf of the member through Premier's group purchasing agreements. Premier also discloses the aggregate vendor payments.

In addition to Premier's vendor grievance process, a vendor may request further review of any outstanding concerns through the Healthcare Group Purchasing Industry Initiative (HGPII) Independent Evaluation Process (https://hgpii.com/what-we-do/). In order to facilitate the HGPII Evaluation, HGPII utilizes the services of the American Arbitration Association® (AAA), an organization that provides alternative dispute resolution services. Premier's vendor grievance process is not intended to waive any rights the vendor or Premier may have related to the enforcement of binding arbitration or any other legal rights and remedies. For the calendar year ending in 2022, there were no grievances filed by suppliers.

Premier may engage in business relationships with participating vendors which include the sale of Premier products and services to participating vendors or any other type of arrangement where money flows from participating vendors to Premier. A participating vendor is a company that has a contract, or submits a formal bid or offer to contract, to provide goods or services to alliance members. These relationships have no bearing on GPO contracting decisions and are publicly disclosed on Premier's company website. This disclosure does not include business relationships that exist to purchase goods and services that are utilized by Premier to carry out its general business operations so long as the terms of the arrangements reflect fair market value for the goods being purchased.

Supplier Diversity

As an organization built on the foundation of transforming healthcare within communities across the country, Premier recognizes that supplier diversity is an important component of our members' success. Diverse suppliers help our hospitals create jobs and improve life in the communities they serve. With the recent hire of Premier's first Chief Diversity and Inclusion Officer, the Supplier Diversity program will remain under the guidance and direction of the GPO; however, the program will be reflected as a pillar under the Diversity, Inclusion and Belonging strategy. We evolve our strategies to continue the focus on socio-economic development and growth of communities through MWBE+ partnerships. The use of program mass will drive better healthcare outcomes, strengthen local economies and develop a more robust supplier diversity ecosystem for the healthcare industry.

Premier's Supplier Diversity Program supports our members by:

- Ensuring diverse suppliers are proactively considered for contracting opportunities.
- Supporting and facilitating procurement from diverse suppliers.
- Encouraging contracted suppliers to support and procure from diverse suppliers.
- Increasing the number of small, diverse and regional enterprises doing business with members of the Premier alliance through Premier's Sourcing Education and Enrichment for Diverse and Small Suppliers (SEEDS) Program.
- Including diverse suppliers in our contract portfolio. In 2022, 12% of Premier's contract portfolio was comprised of diversity suppliers, and included agreements with minority, women, veteran and small business enterprise. In 2021, diverse suppliers were at 10%.

PREMIER®

Premier, Inc. (NASDAQ: PINC) is a leading healthcare improvement company, uniting an alliance of more than 4,400 U.S. hospitals and health systems and approximately 250,000 other providers and organizations to transform healthcare. With integrated data and analytics, collaboratives, supply chain solutions, and consulting and other services, Premier enables better care and outcomes at a lower cost. Premier plays a critical role in the rapidly evolving healthcare industry, collaborating with members to co-develop long-term innovations that reinvent and improve the way care is delivered to patients nationwide. Headquartered in Charlotte, N.C., Premier is passionate about transforming American healthcare.

1 Healthcare IT News. Healthcare breach costs hit record high (July 27, 2022). Available at: https://www.healthcareitnews.com/news/healthcare-breach-costs-hit-record-high. Accessed January 10, 2022
2 U.S. Food & Drug Administration. Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook (November 15, 2022). Available at: https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity. Accessed January 10, 2022