2021

ANNUAL COMPLIANCE REPORT

PREMIER®

Content

Key Highlights For The Year

Alan C. Sauber, Chief Ethics & Compliance Officer

This year's accomplishments demonstrate the continued collaboration between business leaders and the Corporate Compliance department toward achieving Premier's growth goals through a safe and secure process. The team works diligently to keep the company compliant with regulatory and certification needs of the business. Some of the major accomplishments for the year are found below.

- Named one of the World's Most Ethical Companies by Ethisphere® Institute for the fourteenth consecutive year.
- Secured 100% completion of employee annual education and policy attestations for the first three quarters of 2021. Early results for the fourth quarter show a completion rate of 98.6 percent. The remaining 1.4 percent will be completed by January 31, 2022.
- Updated the cybersecurity language in our GPO agreements such that the contracted supplier formally attests to conditions of sale & usage. This ensures manufacturers provide a pre-distribution device designed with the goal of (1) reducing cybersecurity intrusion and misuse; (2) improving availability, reliability and accuracy; and (3) adhering to generally accepted security procedures.
- Updated the Written Information Security Program (WISP) to a robust control framework which accommodates Premier's multiple IT platforms and allows the business to achieve organizational objectives, address new laws, regulations and industry requirements.
- Implemented COMPLOG, an approved secure location for adherence of ITS PHI applications. This ensures that all user access logs contain the necessary information for incident and audit response.
- Implementation of the Incident Response Management tool which has allowed us to better discover data loss and exfiltration by our internal Premier workforce. We developed an entire process, procedure and documentation around this tool to better protect Premier and our customer/member data.
- Updated and improved our annual education via the Privacy Portal to proactively inform and educate Premier's workforce. The tenor of our approach was adjusted to focus on preemptive privacy and security efforts rather than reactive disaster recovery and subsequent mitigation.
- Extensive support of new business activity for Premier Applied Science (PAS). Worked with the PAS team to support early contract engagement of privacy, security and compliance requirements to improve efficiency and provide adequate protection of data rights that are necessary for effective contract negotiations.
- Created a methodology with the GPO Leadership team to develop a business template for the commercialization of data reports as a new source of revenue in response to such requests from our contracted suppliers.
- Completed the first stage of a large-scale contract review project which will identify data rights and restrictions to inform the business of both the strategic growth opportunities and related contractual requirements.
- Successfully completed the Premier Impact Assessment (PIA) audit by KPMG which resulted in improved policies and procedures surrounding Premier's third-party risk management and resulted in a more thorough ongoing monitoring process of our existing vendors based upon the risk they pose to Premier and our customers.

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.

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 sets forth its framework for operating its businesses in an ethical and compliant manner through Premier's Corporate Compliance Program. This program aligns with the Federal Sentencing Guidelines, ensures that policies and internal controls are user friendly, and meets emerging compliance and ethics standards.

Business Rules

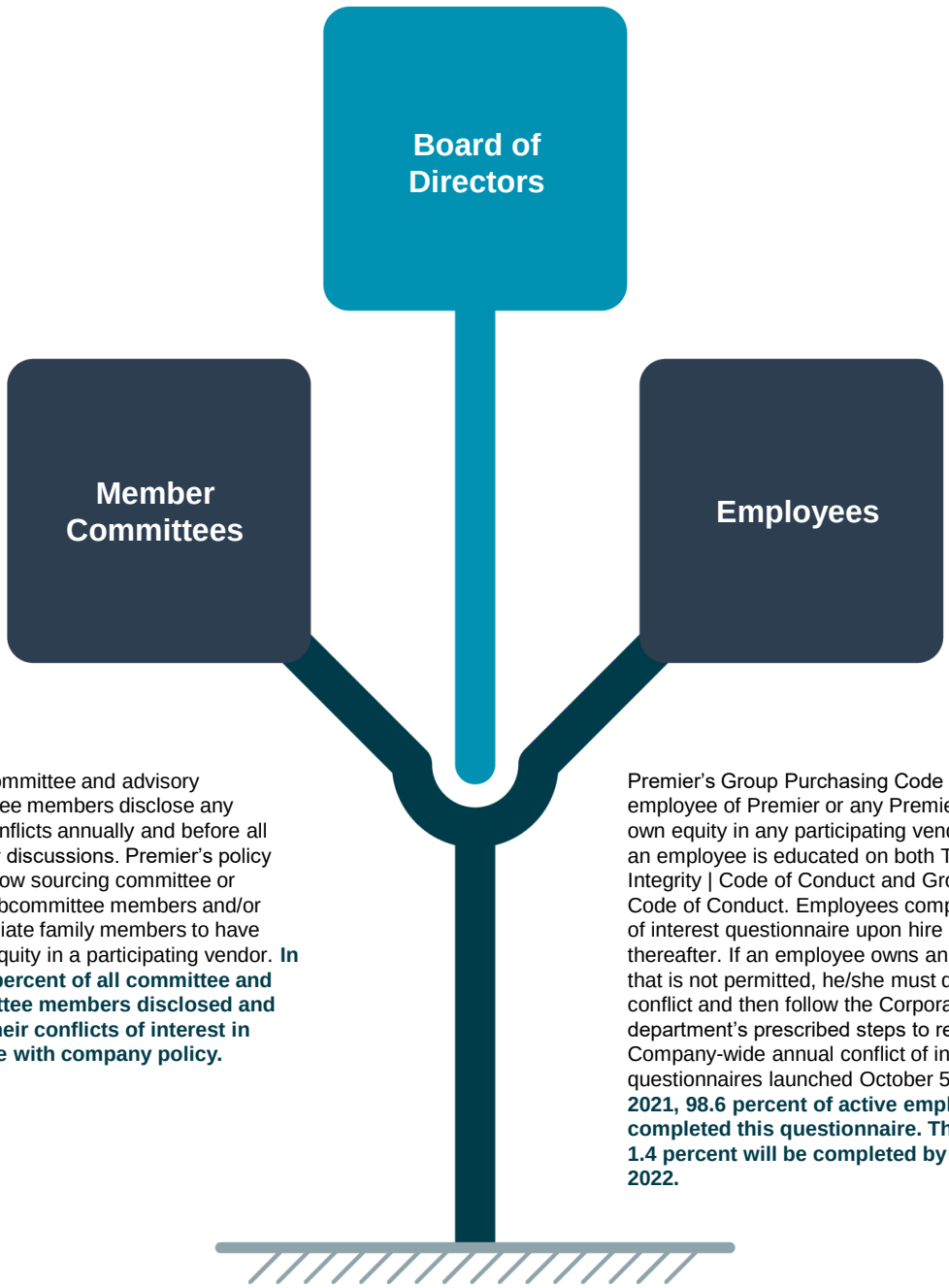
Premier has developed internal business rules for such topics as Administrative Fees, Custom Contracting and other programs that present greater risk to the organization. These rules define how we operate the programs and are verified semi-annually for compliance.

Key Component Areas

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.

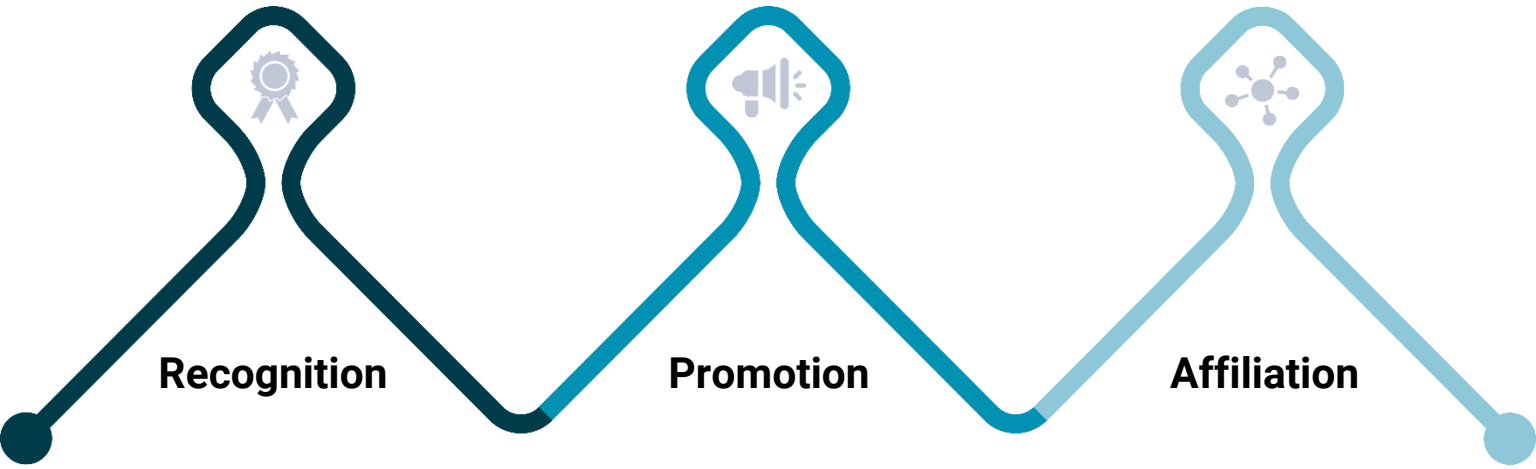
Board members annually disclose potential conflicts that they and/or their immediate family member or related party may have. Conflicts may include affiliation with or managerial, consulting or employment relationships, personal, equity or other financial interests, compensation relationships with any company, vendor or firm and use of non-public information, Premier property and assets. **In 2021, 100 percent of all directors disclosed and resolved their conflicts of interest in accordance with company policy.**



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 2021, 100 percent of all committee and subcommittee members disclosed and resolved their conflicts of interest in accordance with company policy.**

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 5, 2021. **In 2021, 98.6 percent of active employees completed this questionnaire. The remaining 1.4 percent will be completed by January 31, 2022.**

Industry Involvement



For the fourteenth 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 health information services industry recognized this year.

Corporate Compliance was a significant contributor to the development of the company's Environmental, Social and Governance (ESG) program. In September, Premier received the 2021 Diversity Impact Awards™ Top 10 Enterprise-Wide ERG Award for our CDEIB ERG Network.

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, was elected as the incoming chair for the new term. This will help Premier further advance our best practices within our supply chain segment of the business.

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

Privacy

New Privacy Developments

- Significant progress was observed with respect to the passage of comprehensive State privacy laws. Earlier in the year, Virginia became the second state to enact privacy legislation in the form of the Virginia Consumer Data Protection Act ("CDPA") following in the footsteps of California's Consumer Privacy Act of 2018, slated for implementation in January of 2023. In July, Colorado became the third state to enact comprehensive privacy legislation with the Colorado Privacy Act effective July 1, 2023. Lastly, Nevada passed its Act for internet privacy which prohibits data brokers from selling certain consumer information when directed by the consumer and imposes requirements on data brokers when responding to consumer requests.
- Additionally, 2021 continued to see legislation introduced for overarching federal privacy legislation. However, no one comprehensive federal privacy law has passed or been implemented though support is growing for one. For example, the Data Protection Act of 2021, the Data Privacy Act and the Online Privacy Act of 2021 and most recently the Control Our Data Act, a draft bill for a national privacy standard, all have been announced. If officially introduced, these bills would strengthen federal privacy protections and would be guided by core principles which seek to promote innovation, increase transparency and accountability, and set clear rules for protecting consumers' data privacy.
- Health Privacy groups anticipate forthcoming amendments to the HIPAA Privacy Rule which will strengthen patient access rights and enforcement in this area by the US Department of Health and Human Services Office for Civil Rights (OCR). The ultimate purpose of the proposed amendments seek to empower patient rights, improve care coordination and reduce regulatory burdens.
- Finally, the Federal Trade Commission recently reemphasized its commitment to ensuring the protection of sensitive information collected by mobile health apps and made clear that it intends to bring actions to enforce its Health Breach Notification Rule. Under the Rule, vendors are required report a "breach of security" involving personal health records to the FTC, the media (in some cases) and directly to consumers. The FTC also seeks to clarify the scope of entities that are covered by the Rule and clarify the terms used within the Rule. The Rule does not apply to HIPAA covered entities or any other entity to the extent that it engages in activities as a business associate of a HIPAA covered entity.

Premier's Response:

Premier's Privacy team continues to stay informed on proposed state laws and potential federal legislation. As legislation moves forward, the team will analyze the terms and obligations of such proposed laws and appropriately assess their application to Premier's business. In our review, we continue to implement and update our policies and procedures to ensure compliance with the laws and the personal rights of individuals. We continue to collaborate with Premier's Public Affairs team to provide comments and support advocacy efforts for proposed laws and federal bills that may have a detrimental or restrictive impact to Premier's business. We continue to educate Premier's employees on their obligations in regard to the personal information of individuals that Premier receives in the furtherance of its services and solutions. If the amendments to HIPAA are adopted, Premier will need to evaluate our Business Associate Agreement with our customers to ensure our obligations as a business associate relating to access requests are in line with the amended access requirements and other pertinent obligations. We will also need to evaluate our annual HIPAA training and related policies and procedures to account for new obligations and requirements. In regard to the FTC Health Breach Notification Rule, Premier continues to evaluate the applicability of the Rule to Premier's current and future services and solutions.

The SEC and Cybersecurity

The US Securities and Exchange Commission (SEC) has been tough on cybersecurity disclosure controls during 2021 and we expect this trend to continue in 2022. The SEC brought numerous enforcement actions against public companies and SEC-registered financial services providers for deficiencies in cybersecurity disclosure controls and procedures, especially where sensitive personally identifiable information is compromised without appropriate remediation, escalation, and disclosure. Additionally, the SEC has sent numerous letters requesting information from public companies and other SEC-regulated companies potentially impacted by the SolarWinds Compromise. The letters requested information about the December 2020 SolarWinds cyber breach, the impact of the compromise on each recipient, the recipient's response to the SolarWinds compromise, and a broad request asking recipients to identify other compromises involving unauthorized access to the recipient's computer systems by an external actor lasting longer than one day. These activities highlight SEC's ongoing efforts to gather information on vulnerability detection, remediation, and disclosure in the cybersecurity space when the number of ransomware attacks continues to rise.

Premier's Response:

Premier continues to ensure that it closely adheres to the Safeguards Rule and follow the SEC's February 2018 guidance on public company disclosure of cybersecurity risks and incidents. Among other things, Premier's controls and procedures:

- *Set forth steps to identify and investigate cybersecurity incidents;*
- *Assess and analyze the impact of the incident on the company's business and customers;*
- *Ensure careful analysis of whether the cybersecurity incident is material, giving rise to disclosure obligations;*
- *Refer potentially material cybersecurity incidents to appropriate committees for assessment and analysis;*
- *Ensure that material cybersecurity incidents are reported to senior management and to the board of directors;*
- *Ensure that material cybersecurity incidents are disclosed to investors and that existing disclosures are reviewed and, if necessary, updated if new facts render them incorrect or misleading;*
- *Prescribe steps and deadlines to remediate incidents based on severity;*
- *Address circumstances under which trading restrictions should be imposed on company personnel who are in possession of material non-public information (MNPI) regarding the incident; and*
- *Provide for the issuance of a document preservation or litigation hold for material incidents or other incidents where the company anticipates litigation.*

IT Risk Management

The Internet of Things (IoT) is a rapidly evolving and expanding collection of diverse technologies that interact with the physical world. IoT can provide computing functionality and network connectivity for equipment that previously lacked this utility. The full scope of IoT is vast and many organizations are not necessarily aware they are using a large number of IoT devices. These interconnected and internet connected devices can affect their cybersecurity and privacy risks in different ways than traditional information technology (IT) devices.

Securing IoT devices is a major challenge, as manufactures tend to focus on functionality, compatibility requirements, customer convenience, and time-to-market rather than security. Meanwhile, security threats are increasing.

Internet of Things (IoT) Concepts

The Internet of Things consists of the following elements:

- The components (i.e. devices, applications, phones, appliances etc.)
- Components connected / interconnected by a digital network and
- Components communicate with sensors that allow the components to observe, send and receive information about themselves or their environment.

IoT In Healthcare

The Internet of Medical Things (also called the internet of health things) is an application of the IoT for medical and health related purposes, data collection and analysis for research, and monitoring. In the healthcare sector, health IoT gathers, transmits and analyzes data derived from electronic health records (EHR) containing personally identifiable information (PII), protected health information (PHI), patient generated health data, and other machine-generated healthcare data. Health IoT supports services such as real-time monitoring, medication compliance, and imaging.

Medical devices, such as infusion pumps, were once standalone instruments that interacted only with the patient or medical provider. With technological improvements designed to enhance patient care, these devices now connect wirelessly to a variety of systems, networks, and other tools within a healthcare delivery organization (HDO) – ultimately contributing to the Internet of Medical Things (IoMT).

Health IoT Security Objectives

The security objectives of health information technology (HIT) includes implementation of security controls that provide for the confidentiality, integrity, and availability of patient information and for the systems supporting the use and exchange of that information.

The security objectives of medical devices are concentrated around patient safety and focus more on Integrity and Availability. Cybersecurity Risks are different from patient safety risks but they can affect patient safety. The threats and vulnerabilities for cybersecurity risks can be much broader in scope than typical safety hazard, harm, or device failure.

Premier's Response:

Manufacturers can improve the security of their IT products and services by incorporating technical safeguards (i.e., security features) in their devices during the design phase of their product. Risk Management is keeping Medical Device Manufacturers accountable for their role in the Security Management Process by:

- *Strengthening cybersecurity language in our GPO contract template requiring the Contracted Supplier to formally attest they abide by baseline cybersecurity control expectations as conditions of sale/usage. This approach requires manufacturers provide a pre-distribution device designed with the goal of*
  - *(1) reducing cybersecurity intrusion and misuse;*
  - *(2) improving availability, reliability, and accuracy; and*
  - *(3) adhering to generally accepted security procedures, such as the National Institute of Security Standards commonly referred to as NIST*

Regulatory and Compliance

Worked with E&Y in performing the following engagements:

- 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, 2021 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 audit was performed on PremierConnect Enterprise Resource Planning (ERP), PremierConnect Budgeting and Financial Reporting (BFR), PremierConnect Sourcing and Contract Management (SCM), and Contigo Health Total Cost-of-Care Solutions product solutions suite. 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 prima facie evidence of Premier's security hygiene, but also as official attestation from a reputable, objective, and licensed third party that a comprehensive assessment performed based on criteria relative to Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, NIST Special Publication 800-53A, "Security and Privacy Controls for Federal Information Systems and Organizations", and NIST Special Publication 800-53.

Additional Certifications and Assessments

- Completed Premier's 2021 FISMA certification. This annual assessment requalifies Premier to do business with government agencies as a prime contractor.

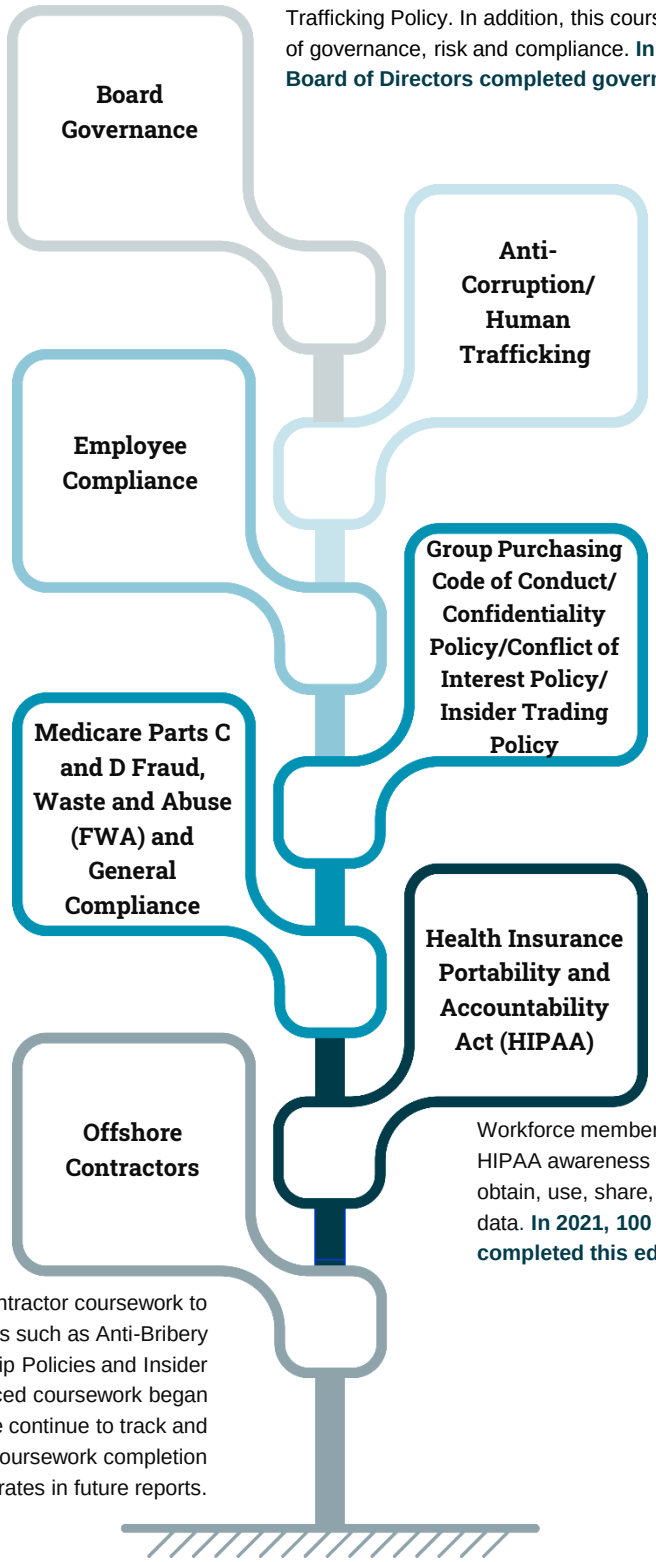
- Performed the necessary assessments for the Payment Card Industry's Data Security Standard (PCI-DSS) for those segments of the business that accept credit cards as payment.

- Continued IT Sarbanes-Oxley (SOX) testing with control owners.

Education

The following is a summary of the compliance educational programming completed in 2021.

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 2021, 100 percent of the Board of Directors completed governance education.**



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: careful communications, ethical leadership, information security, insider trading and social media. **In 2021, 98.6 percent of active employees completed this coursework. The remaining 1.4 percent will be completed by January 31, 2022.**

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 2021, 100 percent of S2S Global employees completed this education.**

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 2021, 100 percent of committee and subcommittee members completed this education.**

As part of Premier's annual compliance education, employees completed online 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 2021, 100 percent of employees completed this education.**

Workforce members completed company-wide HIPAA awareness education on how to properly obtain, use, share, maintain and transfer protected data. **In 2021, 100 percent of employees completed this education.**

Expanded offshore contractor coursework to include policy attestations such as Anti-Bribery Policy, Data Stewardship Policies and Insider Trading Policy. The enhanced coursework began in early November 2021. We continue to track and assess offshore contractor coursework completion and will report completion rates in future reports.

Group Purchasing

COVID-19 Response

Over the course of the COVID-19 pandemic, Premier has worked alongside our members and supplier partners to aggressively respond to the global supply chain challenges. With the support and input of our members, we have made investments in several strategic initiatives and partnerships to improve the resiliency of the healthcare supply chain and to mitigate disruptions within our alliance. Our organization provided thought-leadership and education across a wide range of topics and successfully sought waivers and gave guidance to the US Government in response to member needs and driven legislation in Congress to improve our nation's response to this pandemic and improve preparation for the next one.

As the healthcare supply chain evolves with the continued impact of the COVID-19 variants, we're faced with new challenges and constraints, including rising costs in manufacturing and transportation, labor shortages, domestic supply chain bottlenecks, persistent backorders, and inflation. Premier continues to remain steadfast in our commitment and partnership with members to improve supply chain resiliency and help mitigate disruptions. Premier recognizes that supply chain disruptions are likely to persist well into 2022 and may impact the supply chain longer term.

GPO Code of Conduct

Premier's GPO is governed by a Code of Conduct ("Code") which has experienced relatively few changes since its inception in 2004. To better meet the current market demands and to provide greater clarity, Management, represented by GPO leadership, Legal and Corporate Compliance, convened a working group to condense and update the Code. This resulted in nine major changes to the code that Management presented to the Board for approval in April 2021. The updated Code was approved and is reflected on our public website.

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 2021, 12.5% of Premier contracts had administrative fees above 3% compared to 9.9% in 2020. 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 alliance 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. In its annual financial reporting to alliance members, 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 2021, 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 2021,12% of Premier's contract portfolio was comprised of diversity suppliers, and included agreements with minority, women, veteran and small business enterprise. In 2020, diverse suppliers were also at 12%.

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 225,000 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.