PREMIER® POLICY	TITLE: Confidentiality Policy	
	DATE CREATED: 12/01/2010	VERSION NUMBER: 6
	DATE OF LAST REVIEW: 04/25/2023	DEPARTMENT OWNER: Corporate Compliance

Printed copies are for reference only. Please refer to the electronic copy for the latest version.

1. Purpose

To establish the confidentiality requirements of, and provide guidance for, the protection of Premier Information (as defined herein) obtained during the course of employment.

2. Scope

Applies to all Premier workforce members and the Premier Information accessed, collected, generated, maintained, used and/or entrusted to Premier and Premier workforce members with direct or indirect access to Premier's Information Security Management System, Premier Information Assets and/or is obtained during the course of employment.

3. Definitions

All capitalized terms and related definitions may be found in the *Security and Privacy Violations and Sanctions Policy and Procedure*.

4. Attachments/References

Acceptable Use Policy
Data Stewardship Program
Email and Office Document Labeling, FAQs
FAQ Information Blocking
Information Classification and Retention Policy
Insider Trading Policy
Premier Privacy Portal
Reporting a Suspected Security or Privacy Incident or Violation Policy and Procedure
Security and Privacy Violations and Sanctions Policy and Procedure

POLICY

Premier Information

1. In the course of employment, workforce members may create, receive, know of or gain access to Premier Information (compromised of Premier Internal Information and/or Premier Restricted Information as described in the *Information Classification and Retention Policy*).

2. Premier Information may be in physical form (e.g., paper, e-mail, recording, etc.) and/or may be knowledge acquired through daily work such as from conversations to which one is a party or conversations which are overheard.

Workforce Member Obligations Regarding Premier Information

3. Workforce members must presume that any information about Premier or its customers/members is confidential and therefore must be protected from disclosure and/or misuse.

4. Workforce members are required to safeguard Premier Information, whether generated internally or acquired from other sources, and to use it only in the performance of their employment responsibilities. In particular:
   - 4.1 Workforce members may not personally profit from Premier Information. Workforce members may not use Premier Information to trade securities for their own or related accounts, or to advise relatives, friends or other persons with respect to trading securities. See the *Insider Trading Policy* for more information.
   - 4.2 During and after employment, workforce members may not disclose Premier Information to anyone outside of Premier, nor may workforce members use or permit anyone else to use Premier Information, unless such use or disclosure is directly permitted by the workforce member's employment responsibilities.
   - 4.3 Upon termination of employment, workforce members must return to Premier all physical and electronic copies of Premier Information, as well as all other material embodied in any physical or electronic form that is based on or derived from Premier Information without retaining any copies. Failure to do so may constitute theft and is subject to legal action.
   - 4.4 Workforce members may not seek to obtain Premier Information that is in the possession of other persons or business segments of Premier that is not needed to perform assigned work responsibilities.
   - 4.5 Workforce members must share Premier Information with other workforce members solely as needed for the performance of legitimate job functions.
   - 4.6 Workforce members are required not to leave documents containing Premier Information where such documents may be seen by persons who do not have a need to know the information.
   - 4.7 Workforce members are required to ensure that all Premier Information in a digital format is only viewed on secure devices by individuals permitted to view it.
   - 4.8 Workforce members are required to avoid unnecessary copying and printing of Premier Information. All printed Premier Information must be shredded when the purpose for printing the Premier Information is completed.
   - 4.9 Workforce members are prohibited from sending Premier Information to a personal e-mail account, cloud or any other personal repository.

5. In order to provide Premier Information to any external parties, workforce members must first establish that the party has a legitimate reason to know and ensure that any necessary documentation or legal approval is in place prior to disclosure.

6. Workforce members must comply with the confidentiality obligations that appear in any agreement that applies to them and Premier.

Enforcement

7. Failure to comply with this Policy may, at the full discretion of Premier, result in sanctions, disciplinary or legal actions, and possible termination of employment in accordance with the *Security and Privacy Violations and Sanctions Policy and Procedure*.

8. Certain disclosures of Premier Information in violation of the *Insider Trading Policy* could result in criminal prosecution by the federal government.

9. Nothing in this Policy is intended to interfere with an employee's protected rights under state or federal law, such as communicating with the US Securities and Exchange Commission, Financial Industry Regulatory Authority, U.S. Equal Employment Opportunity Commission, the National Labor Relations Board, the Occupational Safety and Health Administration or any other federal, state or local government agency or commission (including providing documents or other information to such agencies), none of which shall constitute a breach of this Policy. Likewise, this Policy does not prohibit limited disclosure of Premier trade secrets for expressly permissible purposes under the Defend Trade Secrets Act of 2016.

Reporting Unauthorized Disclosures of Premier Information

10. If a workforce member believes that he/she or others have received or disclosed Premier Information inappropriately, such workforce member is obligated to report the concern in accordance with the *Reporting a Suspected Security or Privacy Incident or Violation Policy and Procedure*.

Where to Go with Questions and Concerns

Contact premierprivacy@premierinc.com with questions or concerns about this Policy.