

Pursuant to the Master Agreement or other contract entered into between Supplier and Corewell to which this Payment Card Industry Addendum is incorporated (the "**Agreement**"), Supplier may, in the course of fulfilling its obligations, have access to, use, store, transmit, or process "**Cardholder Data**" and/or "**Sensitive Authentication Data**" (as those terms are defined by the Payment Card Industry Security Standards Council) (collectively "**PCI Data**"). As such, Supplier agrees to the following terms and conditions set forth in this Payment Card Industry Addendum to the Agreement (the "**Addendum**").

1. **Definitions.** Unless otherwise defined in this Addendum, capitalized terms used herein shall have the meaning given them in the Agreement.

"Corewell" means Corewell Health and its subsidiaries, affiliates, and successors.

"Security Incident" means (a) any unauthorized access to or disclosure or acquisition of Corewell's Confidential Information; (b) any act or omission that compromises either the security, confidentiality, or integrity of Corewell's Confidential Information or the physical, technical, administrative, or organizational safeguards put in place by Supplier or by Corewell should Supplier have access to Corewell's systems, that relate to the protection of the security, confidentiality, or integrity of Corewell's Confidential Information; or (c) receipt of a complaint in relation to the privacy and data security practices of Supplier or a breach or alleged breach of this Agreement relating to such privacy and data security practices.

"Supplier" means a vendor, contractor, supplier, or other entity who is providing goods and/or services to Corewell.

2. **Acknowledgment.** Supplier acknowledges that the Corewell data that it may access, use, store, transmit, or process may contain PCI Data. Supplier acknowledges that it is responsible for the security of the PCI Data it possesses, accesses, uses, stores, transmits, or processes.

3. **PCI-DSS Compliance.** Supplier hereby represents, warrants, and covenants that it and its systems are and shall continue to be for the term of the Agreement, compliant with the then-current version of PCI-DSS and such additional regulations, rules, and standards governing PCI Data as may from time to time be adopted by the Payment Card Industry Security Standards Council. Supplier further agrees to:

- i) Comply with all rules and regulations of Visa, Mastercard, American Express, Discover, and any other payment card association or network (each a "**Payment Card Association**"), including Payment Card Industry Data Security Standards ("**PCI-DSS**") and/or Payment Card Industry Software Security Framework ("**PCI-SSF**") or their successor (as applicable) and any other Payment Card Association data security, disaster recovery, or similar programs or requirements ("**Card Association Requirements**"). Supplier is responsible for accurately determining the compliance validation level applicable to Supplier and maintaining compliance in accordance with the then-current Card Association Requirements.
- ii) Promptly: (a) provide to Corewell any other data security reports as required by any Payment Card Association; (b) pay to such Payment Card Association any fines and penalties for any failure of Supplier to comply with any data security requirements; and (c) provide full cooperation and access required by such Payment Card Association to conduct a security review of Supplier's policies and procedures.

4. **Security of PCI Data.** Supplier agrees to keep PCI Data strictly confidential and comply with the PCI-DSS requirements and such additional regulations, rules, and standards governing PCI Data as may from time to time be adopted by the Payment Card Industry Security Standards Council, including: (a) ensuring all PCI Data in Supplier's possession (regardless of form) is secure from unauthorized disclosure; (b) ensuring all PCI Data is, as Corewell elects, either returned to Corewell or permanently, securely, and verifiably destroyed at the end of the business relationship, contract termination, or when no longer needed; (c) ensuring that the PCI Data is only used in furtherance of the performance of services under this Agreement; (d) ensuring a plan is prepared and tested annually to provide for business continuity in case of a major disruption or disaster; and (e) providing the required support and access to allow a PCI-approved third party to complete an audit for compliance with PCI data security requirements.

5. **Reporting Requirements.** Prior to Supplier accessing, using, storing, transmitting, or processing any PCI Data, and on each anniversary of the effective date of the Agreement, Supplier will submit to Corewell a summary of its PCI DSS assessment results and any current or planned remediation efforts in the form of an Attestation of Compliance in accordance with the PCI DSS requirements (which may include a Report on Compliance prepared by a Qualified Security Assessor ("QSA")). Supplier further agrees to provide to Corewell, at least annually, a copy of its PCI DSS responsibility matrix. If applicable, Supplier shall maintain and provide proof of certification by the PCI Security Standards Council of any payment application provided to Corewell or used by Supplier in its provision of the services. If Supplier or any of its representatives becomes aware of a Security Incident or reasonably suspects a Security Incident to have occurred involving PCI Data, Supplier shall immediately, and at its own expense: (i) notify Corewell of the unauthorized access; (ii) cooperate with any Corewell investigation, analysis, notification and mitigation activities; and (iii) indemnify Corewell for all costs it incurs for those activities.

6. **Indemnification.** Supplier agrees to indemnify and hold harmless Corewell, its affiliates, and each of their respective officers, directors, employees, representatives, and agents from and against all costs, losses, liabilities (including regulatory or industry fines), or expenses (including reasonable attorneys' fees), arising out of or related to Supplier's or its affiliates', subcontractors', agents', or employees' breach of this Addendum.

7. **Exclusion from Limitation of Liability.** To the extent that Supplier has limited its liability under the terms of the Agreement, whether with a maximum recovery for direct damages or a disclaimer against any consequential, indirect, or punitive damages or other such limitations, all limitations shall exclude any damages to Corewell arising from Supplier's breach of its obligations under this Addendum.

8. **Termination.** Without limiting any of Corewell's remedies, Corewell reserves the right to terminate the Agreement, upon notice to Supplier, without liability to Corewell, if: (i) a Payment Card Association finds that Contractor has failed to cure any non-compliance with any Card Association Requirements within the timeframe for remediation established by any such Payment Card Association; or (ii) in the event that Supplier has notified Corewell of its non-compliance with any of the requirements related to PCI Data outlined in this Addendum and the parties have not reached a mutually agreeable remediation plan within thirty (30) days of such notification. Any such non-compliance or failure by Supplier will be deemed a material breach under the terms of the Agreement.