

Information Security Terms

1. Purpose. These Information Security Terms (the "InfoSec Terms") are attached to and incorporated by reference to that certain agreement between the Customer and Vertafore, Inc. which governs Customer's use of the applicable Vertafore Solution(s) (the "Agreement"). Capitalized terms used in these InfoSec Terms and not defined in the Agreement are defined herein or in Section 6 below.

Any audit information, policies, and procedures provided by Vertafore to Customer under these InfoSec Terms or the Agreement will be deemed Vertafore's Confidential Information.

2. Information Security Program.

2.1 Vertafore Internal Security Procedures. Vertafore shall implement, maintain, and adhere to the security procedures described herein. Vertafore shall, at a minimum, maintain no less than the levels of security set forth in these InfoSec Terms within Vertafore's facilities where Customer Data is processed, maintained, accessed, or stored.

Notwithstanding the foregoing, the parties acknowledge that best practices, laws, rules and regulations regarding Personal Information or data security may change over time and consequently, Vertafore may modify its practices described in these InfoSec Terms so long as such practices shall not be any less protective than the practices described herein.

2.2 Organization of Information Security. Vertafore shall maintain designated information security and compliance functions for establishing, implementing, monitoring, and improving its information security program. Personnel assigned security responsibilities shall have appropriate authority and organizational access to fulfill those responsibilities.

2.3 Education/Awareness. Vertafore shall maintain a security awareness and training program applicable to personnel with access to Vertafore systems or Customer Data. Training shall be provided during onboarding and periodically thereafter, including at least annually for applicable personnel. Additional role-based training shall be provided as appropriate to personnel responsibilities.

2.4 Background Investigation. Vertafore shall conduct pre-employment background screening for personnel in accordance with applicable law, company policy, geographic requirements, and the sensitivity of the individual's assigned responsibilities. Personnel determined ineligible under applicable company policies shall not be granted access to Customer Data.

2.5 Incident Response. Vertafore shall have an Incident Response Plan ("IRP") in place. The IRP must detail the procedures to be followed in the event of a Security Incident. The IRP will include escalation procedures and a process for notifying the Customer within seventy-two (72) hours. Vertafore shall provide a detailed written report regarding the Security Incident. Initial notification shall include information reasonably available at the time. Vertafore shall provide material updates as additional relevant information becomes available, subject to legal, regulatory, confidentiality, and investigative restrictions. Notification involving a Breach of Unsecured PHI shall comply with the applicable notification requirements established in the Business Associate Agreement and HIPAA.

Vertafore agrees to keep Customer informed of all progress and actions taken in connection with Vertafore's investigation of any Security Incident. Unless such disclosure is mandated by applicable law or regulation, Customer, in its sole discretion, shall determine whether to provide notification to customers, employees, or agents concerning a breach or potential breach involving Personal Information.

2.6 Network Monitoring and Reporting. Vertafore shall maintain security logging and monitoring capabilities appropriate to the risk, functionality, and technical characteristics of systems processing Customer Data. Security-relevant events shall be collected and reviewed through established monitoring and incident response processes. Suspected Security Incidents shall be investigated and escalated according to

Vertafore's Incident Response Plan. Customer notification obligations shall be governed by Section 2.5 and 2.6 and the applicable Agreement.

- 2.7 Right to Audit.** Vertafore agrees to provide assurances in the form of pre-populated industry recognized questionnaires (current year or n-1 SIG or SIG Lite) and provide summaries or artifacts of Vertafore's security policies, standards and physical security controls, at no cost to Customer. Should Customer require a custom questionnaire or assessment, Vertafore may provide such questionnaire or assessments at Vertafore's then-current Professional Services hourly rate, provided that Customer may not request such questionnaires or assessment more than once every twelve (12) months. On-site assessments must be requested with at least thirty (30) days' written notice, and such request may require a statement of work for travel and expenses.
- 2.8 Company Risk Assessment.** Vertafore shall maintain a documented risk management program that includes periodic assessments of information security risks affecting the systems and services used to process Customer Data. Risk assessments shall be conducted based on system criticality, data sensitivity, applicable regulatory requirements, and material changes to the operating environment.
- 2.9 Third-Party Audits.** Vertafore shall conduct, at its own expense, an independent third-party SSAE 18 SOC2 Type II report or SOC3 once every twelve (12) months.
- 2.10 Remediation of Audit Findings.** Vertafore shall use commercially reasonable efforts to remediate audit findings as required by its internal vulnerability management policy.
- 2.11 Asset Management.** Vertafore shall maintain industry standard asset inventory, device management, information classification, handling, and destruction policies and procedures.
- 2.12 Change Management.** Vertafore shall maintain documented change management procedures designed to evaluate, authorize, test, and implement changes to systems supporting Customer Data, as appropriate to the risk and nature of the change. Security impacts shall be considered as part of the applicable change management process.
- 2.13 Requesting and Transferring of Customer Data.** Vertafore shall limit the collection, access, processing, and transfer of Customer Data to information reasonably necessary to provide the contracted services or otherwise authorized under the Agreement. Customer Data shall be transmitted using security measures appropriate to its sensitivity, including encryption where required by applicable policy or law. Where physical media containing Customer Data is transferred, Vertafore shall apply appropriate secure handling, transportation, and tracking controls.
- 2.14 Retention of Customer Data.** Vertafore shall retain Customer Data in accordance with the Agreement, applicable law, documented retention requirements, and established data retention and disposal procedures. Retention and deletion requirements shall account for the operational characteristics of applicable systems, including backup and recovery processes and legally required retention.

3. Information Security Infrastructure.

- 3.1 Access Controls.** Vertafore shall ensure appropriate access controls are in place to protect Customer Data, including the requirements below:
- 3.1.1 Passphrase and Password Requirements.** Vertafore passphrases that grant access to Customer Data shall comply with Vertafore's access control standards. Passphrase and Password complexity must contain the following elements:
- Passphrase and Password length minimums;
 - Passphrase and Password complexity;
 - The ability to restrict use of previously used Passphrase and Password;
 - Passphrase and Password must have an expiry;
 - Account lockout must occur after a maximum number of failed password entry attempts;
 - Minimum account lockout duration after a period of inactivity;
 - Passphrase and Password must not be transmitted or stored in plain text;

- Each user must use a unique username and Passphrase and Password;
- If employees, administrators, or third parties access the network remotely, remote access software must be configured with a unique username, Passphrase and Password, multi-factor authentication, and encryption; and
- Application and operation systems default accounts and Passphrase and Password must be disabled or changed on production systems that support the services provided to Customer prior to Vertafore putting such system(s) into production.

3.1.2 Access Justification/Authorization Process. Vertafore authorization procedures shall comply with the following standards:

- Vertafore shall implement a process that ensures only Authorized Personnel are granted access to Customer Data, and that such authorization is limited to those having a business need in order for Vertafore to fulfill its obligations to Customer under the Agreement.
- Each authorization shall be reviewed by the appropriate management personnel.
- Vertafore shall implement a process that will immediately remove all access to Customer Data for employees that leave the company, or change positions within the company, and no longer require access. If any individual among the Authorized Personnel no longer requires access to Customer Data, Vertafore shall take immediate steps to remove the access of that individual.
- Annual re-verification of individuals that have access to systems that host Customer Data shall be performed to ensure that malicious, out-of-date, or unknown accounts do not exist.
- Vertafore shall ensure that accounts used by third-party vendors for remote maintenance are enabled only during the time needed by that vendor.
- Vertafore shall ensure that group, shared, or generic accounts and passwords are prohibited.

3.1.3 Encryption. Vertafore shall employ encryption and cryptographic protections appropriate to the sensitivity of Customer Data and applicable regulatory requirements. Customer Data shall be protected using industry-recognized encryption mechanisms during transmission over untrusted networks and through appropriate encryption-at-rest controls for applicable storage environments. Encryption mechanisms and key management processes shall be maintained in accordance with Vertafore's established security standards.

3.1.4 System Security. Vertafore shall maintain layered technical security controls appropriate to the risks associated with systems supporting Customer Data. Such controls may include network security protections, endpoint security technologies, vulnerability management, secure configuration standards, and security monitoring. Identified vulnerabilities shall be evaluated and addressed through risk-based remediation procedures consistent with Vertafore's established security policies.

3.1.5 Intrusion Detection. Vertafore shall maintain intrusion detection, prevention, and security monitoring capabilities appropriate to the risk and architecture of its production environments. Such capabilities may include network-level controls, endpoint detection and response, cloud-native security services, and centralized alerting.

3.1.6 Security Logs and Audit Trails. Vertafore shall maintain security logging and monitoring controls for applicable systems processing Customer Data, based on system criticality, security risk, and regulatory requirements. Relevant security events shall be logged and reviewed through established security operations processes. Security logs shall be protected against unauthorized modification and retained in accordance with applicable retention requirements and Vertafore security standards.

3.1.7 Network Segmentation. Vertafore shall implement network and workload segmentation controls designed to restrict unauthorized access between external networks, application services, and data storage environments. Segmentation may be implemented through physical, virtual, cloud-native, or logical security controls appropriate to the applicable solution architecture.

3.1.8 Firewall. Vertafore shall maintain network traffic filtering and access control mechanisms designed to restrict unauthorized network communication. Firewall and equivalent cloud-native security configurations shall be established and maintained through documented configuration and change management processes.

Network security controls shall be periodically evaluated and updated based on business requirements, architectural changes, and identified security risks.

3.1.9 Patch and Vulnerability Management. Vertafore shall maintain a documented vulnerability and patch management program designed to identify, evaluate, prioritize, and remediate security vulnerabilities in applicable systems and software. Remediation activities shall be prioritized based on vulnerability severity, exploitability, asset criticality, exposure, compensating controls, and business risk. Remediation timelines and exceptions shall be governed by established security policies and risk management procedures.

3.1.10 Antivirus and Malware. Vertafore shall maintain malware prevention, detection, and response controls appropriate to the operating environment and associated security risks. Such controls may include endpoint detection and response, behavioral analysis, threat intelligence, cloud-native protections, and other security technologies designed to detect and respond to malicious activity.

3.1.11 System Hardening. Vertafore shall maintain secure configuration and system hardening standards for applicable production systems. Such standards shall address unnecessary functionality, insecure protocols and services, configuration security, and vendor-supplied default settings, as appropriate to the technology and operational requirements of each environment.

3.1.12 Physical Security. Vertafore shall maintain physical security controls appropriate to facilities and equipment under its management that store or process Customer Data. Where Customer Data is hosted by third-party infrastructure providers, Vertafore shall rely on applicable contractual requirements and provider security assurance processes to address relevant physical security obligations.

3.2 Recovery Requirements.

3.2.1 Data Recovery. Vertafore shall maintain documented backup and recovery procedures appropriate to the criticality and architecture of the applicable services. Recovery capabilities shall be designed to support restoration of Customer Data following qualifying disruptions, subject to the technical capabilities, recovery objectives, and service commitments applicable to the contracted solution. Backup data shall be protected through appropriate security controls.

3.2.2 Business Continuity Management. Vertafore shall maintain documented business continuity and disaster recovery processes designed to support the continuation or restoration of critical operations following material disruptions. Plans shall be reviewed periodically and updated as appropriate based on changes to business operations, infrastructure, and identified risks.

3.2.3 Backup Data Storage. Vertafore shall maintain safeguards designed to protect backup Customer Data against unauthorized access, alteration, disclosure, or loss. Backup data shall be secured using appropriate access controls, encryption, monitoring, and retention procedures, based on the applicable backup architecture and security requirements. Where physical backup media is used, additional physical handling, storage, and transportation controls shall be applied as appropriate.

3.3 Information Disposal and Hardware Sanitization. Upon Customer's written request or termination of the Agreement, Vertafore shall sanitize hard drives that contain Customer Data using industry best practices. Data shall be retained for a minimum of sixty (60) days. Paper records containing Customer Data shall be disposed of in a secure manner, including one or more of the following methods: shredding, incinerating, redacting, or otherwise modifying the Customer Data contained in those documents and records to render it unreadable, undecipherable, or unrecoverable, as defined by industry best practices (NIST 800-88, DoD 5220.22-M, or subsequent standards).

3.4 System Development Life Cycle. Vertafore shall maintain documented secure software development practices designed to identify and address security risks throughout the application development lifecycle. Such practices may include secure design principles, architecture and code reviews, automated application security testing, vulnerability remediation, and change management controls, as appropriate to the risk and technical characteristics of the application. Security testing and remediation activities shall be prioritized based on application criticality, data sensitivity, identified vulnerabilities, and applicable security requirements.

4. Personal Information Handling.

4.1 Vertafore shall process Personal Information in accordance with the Agreement and applicable data protection

laws. Vertafore shall not sell Personal Information processed on behalf of Customer and shall not use or disclose such information except as authorized under the Agreement, required or permitted by applicable law, or necessary to provide the contracted services. Where the information constitutes PHI, additional restrictions shall be governed by any applicable Business Associate Agreement.

4.2 Vertafore shall provide reasonable assistance to Customer in responding to requests concerning Personal Information, to the extent required by applicable law and reasonably supported by the functionality and information available within the contracted services. Assistance relating to PHI access, amendment, or accounting requirements shall be governed by any applicable Business Associate Agreement.

5. Precedence. In the event that any provisions of these InfoSec Terms and any provision of the parties' Agreement are inconsistent or conflicting, these InfoSec Terms shall control, but only to the extent of such inconsistency or conflict.

6. Definitions.

Confidential Information	Confidential Information means (a) any non-public information that the Disclosing Party designates as confidential, or which, under the circumstances, ought to be treated as confidential; (ii) any information received by or obtained by the Receiving Party concerning third parties, including without limitation, in the case of Customer, any clients, insureds, customers or claimants of Customer, and/or any subsidiaries or affiliates thereof, and specifically including without limitation any information that Customer is obligated to keep confidential by contract or pursuant to any state or federal privacy laws, including without limitation the Gramm-Leach-Bliley Act (Public Law No. 106-102) (the "Privacy Laws"); (iii) any information relating directly or indirectly to the marketing or promotion of the Disclosing Party's products, the released or unreleased software or other programs of the Disclosing Party, the Disclosing Party's trade secrets, the Disclosing Party's business policies and/or practices, the Disclosing Party's software (in various stages of development), designs, drawings, specifications, models, source code, object code, documentation, diagrams, flow charts, non-public financial information, customer lists and other similar information; and (iv) the Vertafore Solutions.
Customer	The entity listed on the Order which is purchasing Vertafore Solutions from Vertafore. Customer specifically does not include any affiliates, i.e., any entity that directly or indirectly controls, is controlled by, or is under common control with Customer, where "control" means the ownership of more than 50% of an entity's voting securities.
Customer Data	Customer Data means (it) all information entered in software or equipment by or on behalf of Customer and information derived from such information, including as stored in or processed through the equipment or software, (ii) the specifications, designs, documents, correspondence, software, documentation, data and other materials and work products produced by or for Vertafore in the course of its obligations hereunder, (iii) all information concerning the operations, affairs and businesses of Customer or its Affiliates, the financial affairs of Customer or its Affiliates, and the relations of Customer or its Affiliates with its or their employees and service providers (including customer lists, customer information, account information and consumer markets), (iv) software and other intellectual property provided to Vertafore by or through Customer or its Affiliates (if applicable), including third-party software, in object code and/or source code form, (v) all personally identifiable information of Customer's clients, employees and individuals acting as suppliers to Customer, and (vi) other information or data entered into applications, networks or systems as a part of or incidental to the provision of the Services, stored on magnetic media or otherwise

or communicated orally, and obtained, received, transmitted, processed, stored, archived or maintained by Vertafore under this Agreement.

Ineligible Personnel	
Personal Information	As defined by the applicable regulation or otherwise individually identifiable information about a person, including personal, health and financial information.
Security Incident	Any verified, actual, and unauthorized access to or use of Customer Data, including disclosure, theft or manipulation of information that has the potential to cause harm to Customer systems, information, or the Customer brand name.
Vertafore Solution	Collectively, all products and services provided by Vertafore to Customer, including, but not limited to In-House Software, Online Services, Maintenance, and Professional Services.