Vertafore

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 have information security and compliance organizational functions which clearly define information protection roles, responsibilities, and accountability. Vertafore shall define, document, and assign ownership to oversee development, adaptation, and enforcement of information security and compliance requirements, policies, standards, and procedures. Assigned personnel must have the authority within the organization to execute the information security and compliance responsibilities in an effective and independent manner.

2.3 Education/Awareness. Vertafore shall use reasonable efforts to ensure that all employees, subcontractors, agents and other parties acting on behalf of Vertafore ("**Authorized Personnel**") are aware of and comply with Vertafore's security policies. All Authorized Personnel must participate in security awareness training at least annually and new Authorized Personnel must undergo training prior to accessing Customer Data.

2.4 Background Investigation. Vertafore's hiring practices shall include a complete background check. Such background checks shall include: (1) social security number validation; (2) review of government sanction registries; and (3) review of county felony and misdemeanor criminal history records of all counties the individual has resided in within the prior seven (7) years. Ineligible Personnel will not be permitted to perform services that grant 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.

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. For all applications and systems associated with the access of Customer Data, Vertafore shall generate audit logs detailing use and access. Vertafore shall notify

Customer in the event that a review of the audit logs reveals reasonable evidence of a Security Incident.,

Vertafore shall investigate suspected Security Incidents involving Customer Data. In the event of a Security Incident, Vertafore shall, within three (3) business days, notify Customer and provide detailed written information regarding the Security Incident.

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 conduct, at its own expense, an annual risk assessment of all information systems associated with any access of Customer Data.

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 and follow industry standard change management procedures. Vertafore shall use commercially reasonable efforts to ensure that any changes to systems do not negatively impact the security of Customer Data.

2.13 **Requesting and Transferring of Customer Data.** Vertafore shall request only such Customer Data as is necessary to perform its obligations under the Agreement. The processes for data transmission between Customer and Vertafore will be designed and implemented to use the least Customer Data necessary.

All handling and physical transfer of Customer Data shall be carried out using best industry methods appropriate to the sensitivity and criticality of the information. The process for the handling and physical transport of Customer Data must be documented. Upon Customer's written request and within thirty (30) days of physical transport, such documentation will be made available to Customer for review onsite at the applicable Vertafore location. Appropriate physical controls include professionally trained security personnel, Closed Circuit Television (CCTV) of transportation and processing facilities, secured lock boxes and extensive tracking, and auditing of all packages containing Customer Data. Such physical security standards shall be required of any third-party contractor hired for transportation or storage of Customer Data offsite.

2.14 Retention of Customer Data. Vertafore shall work with Customer to meet mutually agreeable retention requirements.

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.

3.2 Encryption. Encryption shall be required if Customer Data is transmitted over public networks, or the use of encryption is mandated by law or regulation. Where Customer Data is transmitted over public networks or over private or public wireless networks, Vertafore shall use strong cryptography

and encryption techniques to safeguard sensitive Customer Data. Vertafore shall not permit wireless access points in the production environment that hosts Customer Data.

3.3 **System Security.** Vertafore shall have commercially reasonable network intrusion detection, firewalls and anti-virus/anti-malware protection in place. Vertafore shall ensure that all systems that are associated with Customer Data are patched within a commercially reasonable time period after Vertafore has actual or constructive knowledge of any security vulnerabilities. Vertafore will take commercially reasonable steps to ensure that any software, systems, or networks that may interact with Customer's systems or Customer Data do not become infected by any computer viruses or other harmful components. System hardening and configuration requirements shall meet industry standard practices.

3.4 **Intrusion Detection.** Vertafore shall implement intrusion prevention systems to monitor all network traffic associated with access, processing, storage, communication, and transmission of Customer Data. Authorized Personnel will be alerted to suspected compromises and must keep all intrusion prevention systems up to date.

3.5 **Security Logs and Audit Trails.** Vertafore shall ensure that all systems storing, or processing Customer Data have logging enabled to a respective log system or a centralized log server. Vertafore shall actively monitor logs to identify suspected unauthorized or malicious activity to facilitate incident response. Vertafore shall maintain logs in alignment with the Vertafore Record Retention Schedule.

3.6 **Network Segmentation.** Vertafore shall implement a DMZ to filter and screen all traffic to prohibit direct routes for inbound and outbound Internet traffic. Customer Data will be logically or physically segregated, prohibiting direct public access between external networks and any system component storing Customer Data.

3.7 **Firewall.** Vertafore shall establish firewall configuration standards including:

- A formal process for approving and testing all external network connections and changes to the firewall configuration;
- A requirement that existing firewall configuration will be periodically reviewed;
- Descriptions of groups, roles, and responsibilities for logical management of network components;
- A firewall configuration that denies all traffic from "untrusted" networks/hosts except required to support Vertafore services;
- A firewall configuration standard that restricts connections between publicly accessible servers and systems that contain Customer Data;
- Implementation of IP masquerading to prevent internal addresses from being translated and revealed on the Internet; and
- Restriction of inbound and outbound Internet traffic to IP addresses with a DMZ (ingress filters).

3.8 **Patch and Vulnerability Management.** Vertafore shall ensure that all system components and software have the latest vendor-supplied security patches, using a risk-based approach, within commercially reasonable timeframes as required by its internal vulnerability management policy. Vertafore shall maintain intelligence feeds or processes to identify newly discovered security vulnerabilities (e.g., subscribe to alert services freely available on the Internet) and shall update standards to address new vulnerability issues.

3.9 **Antivirus and Malware.** Vertafore shall install and maintain antivirus software to protect Customer Data from viruses, worms and other damaging programs. Virus-screening software shall be

maintained on all systems that access Customer Data. Antivirus software must be regularly updated with virus signatures in order to protect against new viruses.

3.10 System Hardening. Vertafore shall implement industry best practices with respect to system hardening on systems hosting Customer Data including:

- Removing all unnecessary system functionality including scripts, drivers, features, subsystems, and file systems;
- Disabling all unnecessary and insecure services and protocols;
- Configuring system security parameters to prevent misuse; and
- Changing vendor supplied defaults before the system is live on the network.

3.11 Physical Security. Vertafore shall ensure that physical security measures are in place to control physical access to any systems and records that contain Customer Data. For so long as the Vertafore is in possession of Customer Data, Vertafore shall physically store all records and media containing Customer Data in an area where access can be limited to Authorized Personnel only.

3.12 Recovery Requirements.

3.12.1 Data Recovery. Vertafore shall have the ability to recover Customer Data in the event of a disaster. Vertafore shall have a written policy ("**Data Recovery Policy**"), covering back up copy procedures for Customer Data. For the term of the Agreement, and at all times while in possession of Customer Data, the Company shall maintain the Data Recovery Policy, and shall safeguard the back-up copies in accordance with such Data Recovery Policy, using the same format and a method at least as secure as the Data Recovery Policy format and methods.

3.12.2 Business Continuity Management. Vertafore shall maintain a written business continuity plan, to support continued business operations in the event of a business disruption or disaster declaration. The business continuity plan will be reviewed periodically, but no less than once every twelve (12) months.

3.12.3 Backup Data Storage. Vertafore shall adhere to the security measures stated in these InfoSec Terms to secure backup Customer Data. Vertafore shall:

- Store media backups containing Customer Data in secure storage, which may be either a third-party or a commercial storage facility;
- Maintain strict control over the internal or external distribution of any media backups that contain Customer Data;
- Encrypt all backups of Customer Data;
- Send media backups via secured courier or a delivery mechanism that can be accurately tracked;
- Require management approval of all media backups that are moved from a secured area, particularly when media backups are distributed to individuals;
- Store paper records in a secure manner; and
- Maintain a list of all records and backup media stored.

3.13 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 but will be stored for no more than one (1) year from the date of termination. 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).

3.14 **System Development Life Cycle.** Applications transmitting Customer Data must use a System Development Life Cycle ("SDLC") framework methodology that encourages secure application design and development. These activities include design review, architecture analysis, and application security scanning. Vertafore shall ensure that proper change control procedures, which will comply with Information Technology Infrastructure Library("ITIL") standards, are enacted.

4. Personal Information Handling.

4.1 Vertafore agrees that it shall not sell Personal Information that is inputted into Vertafore Solutions and Vertafore shall not retain, use, or disclose the Personal Information inputted into Vertafore Solutions for any purpose other than for the purposes outlined in the parties' agreement or as permitted by applicable law.

4.2 Vertafore agrees to assist Customer in responding to any privacy request by a consumer pursuant to applicable laws as is necessary.

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	Any person who has been convicted of any felony within seven years prior to employment with Vertafore or of any misdemeanor criminal offense that demonstrates a breach of trust.
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.