January, 2016

SPECIFIC SOLUTIONS, INC.

HIPAA PRIVACY AND SECURITY GUIDELINES

SPECIFIC SOLUTIONS, INC.

PRIVACY & SECURITY POLICY

Specific Solutions, Inc. is committed to protecting the privacy of our agents and their clients. To provide the products and services expected from a top financial brokerage firm, we must collect personal information about our agents' clients. **We do not sell any personal information to third parties**. We share clients' personal information with the appropriate insurance carriers as necessary to provide the products or services requested. This notice describes our current privacy practices. As our relationships with clients and agents continue, we will update and distribute our Privacy Practices as required by law. Even after relationships end, we will continue to protect the privacy of all personal information.

INFORMATION WE MAY COLLECT AND USE

We collect personal information about our clients to help us identify them from other customers; to process requests and transactions; to offer insurance services; or to tell our agents about products or services that clients may want and use. The type of personal information we collect depends on the products or services requested and may include the following:

Information from the client: The client provides their information when submitting an application, such as name, address, social security number; and financial, health and employment history.

Information about your transactions: We keep information about the transactions with us, such as the products a client purchases and the amount paid.

Information from outside our company: When a client is purchasing insurance products, with their authorization, we may collect information from other individuals or businesses, such as medical information and in force policy information.

HOW WE USE PERSONAL INFORMATION

We may share personal information within our company, certain service providers and with insurance carriers of the clients' choice. They use this information to process transactions the client has requested; provide customer service; and inform our agents of the products and services we offer that would best fit their clients. Our service providers may or may not be affiliated with us. They include financial service providers (for example, insurance agents and brokers, re-insurers, and financial service companies). Our service providers also include non-financial companies (for example, vendors and companies gathering information on our behalf). Information obtained from a report prepared by a service provider, may be kept by the service provider. We require our service providers to protect all client personal information and to use or disclose it only for the work they are performing for us, or as permitted by law.

WHAT INFORMATION WE DISCLOSE

We do not disclose nonpublic personal information about our current or former customers to any non-affiliated entity, except as permitted by law. Examples of the disclosures which we are permitted by law to make include: disclosures necessary to service or administer an insurance or annuity product that you requested or authorized; disclosure made with your consent or at your direction; disclosure made to your legal representative; disclosures made in response to a subpoena or an inquiry from an insurance or other regulatory authority; disclosures made to comply with federal, state or local laws and to protect against fraud.

CONFIDENTIALITY OF MEDICAL INFORMATION

We understand clients may be especially concerned about the privacy of their medical information. We do not sell or rent client medical information to anyone; nor do we share it with others for marketing purposes. We only use and share client medical information for the purpose of underwriting insurance.

SECURITY OF INFORMATION

Keeping information safe is one of our most important responsibilities. We maintain physical, electronic and procedural safeguards to protect all client information. Our employees are authorized to access client information only when they need it to provide a client with products or services they have requested. Employees who have access to personal information are required to keep it strictly confidential. We provide training to our employees about the importance of protecting the privacy of all client information.

Specific Solutions' email server is set up to communicate via Transport Layer Security (TLS) for both inbound and outbound email.
Transport Layer Security (TLS) is a protocol that guarantees privacy and data integrity between client/server applications communicating over the internet. The TLS protocol is made up of two layers: The TLS Record Protocol – layered on top of a reliable transport protocol, such as TCP, it ensures that the connection is private by using symmetric data encryption and it ensures that the connection is reliable. The TLS Record Protocol also is used for encapsulation of higher-level protocols, such as the TLS Handshake protocol. The TLS Handshake Protocol – allows authentication between the server and client and the negotiation of an encryption algorithm and cryptographic keys before the application protocol transmits or receives any data.

Questions about personal information should be directed to:

SPECIFIC SOLUTIONS, INC.
Attn: Management Team
475 International Dr.
Williamsville, NY 14221

BE AWARE OF PHISHING EMAILS

Specific Solutions will never send an unsolicited email to you asking you to verify or update your personal or account information. If you receive an email that appears to be from Specific Solutions and it asks you to respond by providing personal or financial information, do not reply or click on the link. Instead, contact Specific Solutions directly to confirm the legitimacy of the email.

SPECIFIC SOLUTIONS WEBSITE

Is not password protected, and is open to the general public. Agents may access their case status on line, which is password protected to their own individual password. Specific Solutions Administrative team will maintain records of each producers sign on information for the purposes of security.

INFORMATION COLLECTED DURING WEBSITE VISITS

Like most online sites, ours may automatically collect information about your computer hardware and software which include your browser type, operating system, access times and your IP address. This information is often contained in "cookies" that filter the content we present to you to make it easier to navigate the site, for example, to filter content based on your state of residence, and to help us determine which parts of our sites people are visiting.

Data that tracks use of our websites, tools and features is typically collected by a contracted third-party service provider acting on behalf of Specific Solutions. The data is collected in aggregated form only, and not used in a manner that will allow us to identify you.

Third parties may not collect personal information about your online activities over time and across different Specific Solutions web sites or online services for their own purposes.

LINKS TO OTHER WEBSITES

We are not responsible for the information collection practices of other Web sites when you link to them from our Web site. We cannot guarantee how those parties use cookies or whether they place on your computer cookies that may identify you personally. You should carefully review the privacy policies of each Web site you visit to understand how they collect, use, and disclose information.

SAFEGUARDS

Administrative:

Our Agency Management Team is responsible for all privacy & security concerns along with the administration of these policies. Our company requires all new employees to sign our privacy & security training packet as part of their orientation. We also conduct an annual privacy & security training session. Each employee also signs an employee handbook, which confirms they've learned and understand the privacy & security agreement within our agency.

Upon termination of a Specific Solutions employee, the employee is required to leave all property of Specific Solutions at their workstation. All terminated employee computer ID's and passwords are eliminated from our computer system immediately.

Employees are instructed to protect all client personal information. Personal information is always sent through secure channels to the necessary insurance carrier. In event of a security breach, Specific Solutions' management is notified immediately.

Physical:

Business hours of operation are from 8:30am to 5:00pm. During this time Specific Solutions management is on the premises. One main entrance is open to guests with staff being present to direct them accordingly. All other entrances are locked securely and only accessible with a key provided by Property Management. All doors to the office space are closed and locked by 5:00pm. Only employees with a key can access the space after this time.

Only Specific Solutions employees have IDs and passwords to the computer system along with our IT provider and Specific Solutions management. Passwords are required to be changed every 60 days.

Employees will nightly clear their workspace and lock up confidential paperwork in desk drawer, overhead compartment, file cabinet, or locked storage room.

Applications and documentation is scanned in to a password protected file system. Paper documentation is then locked in a confidential shred bin and disposed of on a monthly basis or as needed.

All incoming and out going mail is reviewed by designated employees of Specific Solutions and distributed accordingly.

***Technical*:**

Each username and password is established with the necessary access levels for the employee to do their job. Our server is behind a secure firewall and all laptops have Symantec software and are password protected. The systems are shutdown at the end of each workday and are backed up with tapes removed by management each evening and returned the following morning. Any and all system privileges can be revoked immediately.

All incoming correspondence to the fax machine is picked up and distributed as they come in. Fax machines are in a separate area, which is locked at the end of the business day.

Our server room and any additional technology equipment, CDs, DVDs are stored in a locked room.

We do not allow protected personal information to be transmitted through mobile devices or e-mail, and our Wi-Fi signal is protected and can only be utilized with direct programming.

All hard drives will be removed from copiers when they are being replaced.

Personal cell phone usage, for any purpose, is never permitted in the work areas. Cell phones are to be in the off position when coming into this office, they are to be kept out of sight, and are to remain so until leaving this office. We will strictly enforce no cell phone usage.

Any information contained or used from USB devices is the sole property of Specific Solutions.

CONFIDENTIALITY AND COMMUNICATION POLICY

All employees, associates, and/or agents affiliated with Specific Solutions are required to follow the written confidentiality agreement to protect the personal information of our clients. As an affiliate of Specific Solutions, you may come in contact with and have access to confidential and proprietary information of the Company including but not limited to customer records, sales information, insurance information, client lists, product lists, accounting records, applications, insurance in force, surrenders, changes of benefits, loans, or any other business. Protecting such information is the responsibility of each individual because we all share a common interest in making sure it is not improperly or accidentally disclosed. Do not discuss the confidential and/or proprietary information with anyone who does not work for Specific Solutions. Employees and agents should make no public statements concerning such information.

All records, procedures, sales information and confidential company information developed or used by you while affiliated with Specific Solutions remain the property of the company. No files or copies thereof may be removed from the Company without permission from the Owners of the Company.

CONFIDENTIALITY NONDISCLOSURE AGREEMENT

This Confidentiality Nondisclosure Agreement ("Agreement") is between Specific Solutions, Inc. and _____, (Agent, Employee, or Third Party).

Whereas in the course of transacting business between the parties hereto, it may be necessary for either party to disclose propriety or confidential information, the parties hereto agree as follows:

All information and documents given to the other party shall be considered either proprietary or confidential, whether or not marked as such, and shall be subject to the terms of this Agreement.

Therefore, in consideration of each party making the confidential information available to the other party, the parties agree as follows:

I. Each party warrants that it will retain all information belonging to the other party in strictest confidence and will neither use it nor disclose it to a third party, other than its employees having a need to know, without the explicit written permission of the other party

II. Each party will limit the number of copies made of such information to those necessary and will reproduce a legend as to confidentiality or secrecy on each copy.

III. Each party will require its employees to whom confidential information has been disclosed to keep it in strictest confidence.

For purposes of this Agreement, proprietary and confidential information will include all internal business practices, software, information contained on LANS, computers or other magnetic media, devices, concept, procedures, information plans, strategies, business records, including but not limited to information concerning members, providers, reimbursements, rates, products, pricing, the identity of agency's customers, any and all data identifying agency customers either individually or as a group, including but not limited to, rating, health information, and identifiable nonpublic personal information, agency's methods of doing business, and financial information regarding agency's customer contracts, both detailed information and the basic nature of the information, and contracts or business methods in any form whatsoever.

The parties recognize that irreparable harm can be occasioned to the other party by disclosure of information relating to its business and any violation of the Agreement shall entitle the offended party to injunctive relief in addition to, and not in lieu of, any damages to which the offended party may be entitled. If confidential property or proprietary information is disclosed to a third party, the offending party will provide all reasonable assistance to the other party in obtaining retrieval of the information and shall hold harmless and indemnify the non-offending party from any claims, actions, or suits arising out of the violation of this Agreement.

Notwithstanding anything to the contrary, neither party shall have an obligation to preserve the confidentiality of any information which:

(i) has been previously published or is now or becomes public knowledge through no fault of the other party:
(ii) at the time of disclose is already in the lawful possession of the other party;
(iii) was made available to the other party, without restriction on disclosure, by a third party not under obligation of confidentiality with respect to the disclosed information;
(iv) is independently developed by the other party;
(v) constitutes know-how which in ordinary course becomes indistinguishable from the know-how of the other party;
(vi) the communication is in response to a valid order by a court of competent jurisdiction or otherwise required by law.

At the termination of the relationship requiring the disclosure of proprietary and confidential information, Consultant will promptly, upon the request of Agency, destroy all documents or other matters furnished hereunder constituting or containing proprietary or confidential information (including all electronic information or images of same), without retaining any copy thereof. Consultant shall certify in writing to Agency that all proprietary and confidential information, which had been disclosed to Consultant hereunder has been destroyed.

The validity, construction and performance of this Agreement and the legal relations among the parties to this Agreement shall be governed by and construed in accordance with the laws of the State of New York without giving effect to its conflict of law principles. The parties agree that the courts of Erie County shall be the exclusive courts of jurisdiction and venue for any litigation, special proceeding or other proceeding as between the parties that may be brought, or arise out of, or in connection with, or by reason of this Agreement and each party hereby irrevocably consents to the jurisdiction of such courts for the limited purposes stated herein. If any provision of this Agreement or the application of any such provision shall be held by a tribunal of competent jurisdiction to be contrary to law, the remaining provisions of this Agreement shall continue in full force and effect.

This Agreement constitutes the entire agreement between the parties in connection with the subject matter hereof and supersedes all prior and contemporaneous agreements, understandings, negotiations and discussions, whether oral or written, of the parties and/or subsidiaries of the parties with respect to the same subject matter hereof. There are no warranties, representations and/or agreements between the parties in connection with the subject matter hereof except as specifically set forth or referred to herein.

IN WITNESS WHEREOF, and intending to be legally bound hereby, the parties have caused this instrument to be duly executed as of the date above written.

ACCEPTED BY SPECIFIC SOLUTIONS:

BY: _____
(Signature)

_____
(Printed Name)

_____
(Title)

_____
(Date)

ACCEPTED BY:

BY: _____
(Signature)

_____
(Printed Name)

_____
(Title)

_____
(Date)

PRIVACY & SECURITY TRAINING

All employees of Specific Solutions, Inc. will participate in an annual Privacy & Security training program. Training will be held the first quarter of every year and will be posted on the monthly calendar.

The training contents will include:

1. Review of Specific Solutions' Privacy & Security Policy
2. Review of Specific Solutions' Confidentiality Agreement
3. Office Guidelines and Safeguards
4. E-mail/Fax/Snail Mail Policies
5. Clean Desk Policy
6. Steps to reporting a Security Breach

OUR OBLIGATION

We are required by law to maintain the privacy of your personal information, give you notice of our legal duties and privacy practices, notify you following a breach of your personal information, and to follow the terms of the notice currently in effect. We may change the terms of this notice at any time. The revised notice will apply to any personal information we maintain. Once revised, we will post it on our website.