



**HIPAA PRIVACY AND SECURITY GUIDELINESS**

I. Privacy & Security Policy..... 1  
II. Safeguards..... 3  
III. Confidentiality Agreement.....4  
IV. Privacy/Security Breach Procedure .....7  
V. Return/Destruction of PHI Procedure.....8  
VI. Privacy Security Training ..... 9

## **PRIVACY & SECURITY POLICY**

KAFL Incorporated is committed to protecting the privacy of our agents and their clients. To provide the products and services expected from a top financial services 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 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.

**Information from your employer:** If an employer purchases group products from us, we may obtain information about a client from their employer in order to find the appropriate plan for the business.

### **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, reinsurers, 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.

## **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.

Questions about personal information should be directed to:

KAFL, Incorporated  
Attn: Management Team  
800 Linden Avenue  
Rochester, NY 14625-2710  
585-271-6400

## **SAFEGUARDS**

### *Administrative:*

Our Agency Management Team is responsible for all privacy & security concerns along with the administration of these policies. We also conduct an annual privacy & security training session. Each employee signs an employee handbook which confirms they've learned and understand the privacy & security agreement within our agency.

Upon termination of a KAFL employee, the employee is required to return the office access tag immediately. If the terminated employee leaves without returning the key tag, the Director of Operations can contact the Property Management Company and disable the tag immediately. All terminated employee computer ID's, remote access and passwords are immediately eliminated from our computer systems.

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 KAFL Management is notified immediately along with our security contacts at specified insurance carriers.

### *Physical:*

Business hours of operation are from 8:30am to 5:00pm. During this time KAFL management is on the premises. One main entrance is open to guests and a receptionist directs them accordingly. All other entrances, with the exception of our main entrance, are locked securely and only accessible with a "key fob" provided by KAFL Management. All doors to the office space are closed and locked by 5pm. Only employees with a key fob can access the space after this time. Only KAFL employees have Ids and passwords to the computer system.

Employees clear their workspace and lock up confidential paperwork in desk drawers. Applications and documentation are scanned into a password protected online file system. Paper documentation is then locked in a confidential shred bin and disposed of on a bi-monthly basis or as needed. All incoming and outgoing mail is reviewed and distributed accordingly. Our agency utilizes thick, white envelopes for mailing.

### *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 Small Business Endpoint and are password protected. All outside business laptops have encrypted drives and are protected with LoJack. The systems are locked at the end of each workday. Any and all system privileges can be revoked immediately. All incoming correspondence to the fax machine is distributed as they come in. 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. Any emailed non-public information is sent securely. Our Wi-Fi is public access only and does not integrate with our protected network.

## **CONFIDENTIALITY AND COMMUNICATON POLICY**

All employees, associates and/or agents affiliated with KAFL Incorporated are required to follow the written confidentiality agreement to protect the personal information of our clients. As an affiliate of KAFL 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 KAFL, Inc. 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 KAFL 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”) between KAFL Incorporated 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 proprietary 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 LANSs, computers or other magnetic media, devices, concepts, 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 for 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 this 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 Monroe 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 KAFL:**

**ACCEPTED BY:**

BY: \_\_\_\_\_  
(Signature)

BY: \_\_\_\_\_  
(Signature)

\_\_\_\_\_  
(Printed Name)

\_\_\_\_\_  
(Printed Name)

\_\_\_\_\_  
(Title)

\_\_\_\_\_  
(Title)

\_\_\_\_\_  
(Date)

\_\_\_\_\_  
(Date)

<b>KAFL, Incorporated</b>	Reporting of Suspected Privacy/Security Breach	
<b>Approved By: KAFL Inc.</b>	<b>Date:01/2007</b>	<b>Next Review Date: 11/2019</b>
<b>Policy Type:</b>	<b>Policy #:</b>	<b>Page 1 of 1</b>
<b>Review/Revision Date: 1/1/18</b>	<b>Revision Approval By: LG</b>	

**Purpose:**

This document is to provide guidelines on the required reporting of suspected or actual privacy and /or security breaches of protected health information in accordance with Privacy & Security Agreement.

**Policy:**

This procedure follows the guidelines documented in KAFL’s Policy on Confidentiality of Protected Personal Information and as described in the Privacy & Security Policy.

**Reference:** Notification of Breach Report Form

**Procedure for Employees:**

1. Identify a suspected privacy or security breach of protected health information.
2. Contact KAFL Management Team and together investigate incident to collect all information required to complete the Notification of Breach report form.
3. Submit Notification of Breach Report Form Humana.
3. Receive notification of acceptance of Notification of Breach report form or receive returned Notification of Breach report form with request for additional actions to rectify incident.
5. Follow actions requested to rectify breach incident.
6. If additional corrective actions are requested, items will be reviewed by the KAFL Management Team and implemented.
7. Management will sign Notification of Breach report form acknowledging receipt and agreement of additional corrective actions needed.



<b>KAFL, Inc.</b>	Return/Destruction of Protected Health Information upon Contract Termination	
<b>Policy Type:</b>	<b>Policy #:</b>	<b>Page 1 of 1</b>
<b>Approved By: KAFL Management</b>	<b>Date:01/2007</b>	<b>Next Review Date: 01/2019</b>
<b>Review/Revision Date: 1/1/2018</b>	<b>Revision Approval By: LG</b>	

**Purpose:**

This document is to provide guidelines on the required return or destruction of protected health information (PHI) upon termination of Contract in accordance with Privacy & Security Agreement.

**Policy:**

This procedure follows the guidelines documented in KAFL’s Policy on Confidentiality of Protected Personal Information and as described in the Privacy & Security Policy.

**Reference:** General Agency

**Procedure for Employee:**

1. Upon termination of the Contract for any reason, contact will be made with KAFL to discuss the return or destruction of PHI that was received from KAFL or created or received by the employee.
2. Follow instructions provided by KAFL to return or destroy the PHI.

**\*NOTE:** If return or destruction is not immediately feasible, the Employee shall continue the protection of the data pursuant to the requirements outlined in the Privacy & Security Agreement and limit the further use of PHI until return/destruction has occurred.

## **PRIVACY & SECURITY TRAINING**

All employees of KAFL, Incorporated will participate in an annual Privacy & Security training program. Training will be held every year.

The training contents will include:

1. Review of KAFL's Privacy & Security Policy
2. Review of KAFL's 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