IFG SPECIFIC - INFORMATION SECURITY PLAN

DEFINITIONS

Please carefully review the definition of these terms, because they are used frequently in this plan:

"Plan" refers to the Information Security Plan.

"Agency" refers to MDA Insurance & Financial Group, Inc.

"Clients" refers to the Agency's clients, former & prospective clients.

"Encrypted" refers to the use of a program to put computer data into a coded format that cannot be read by unauthorized users.

"Passwords" refers to a string of characters that, when possible, is at least 8 characters long and contains at least three of the following: upper case letter, lower case letter, a number, a special character (%, &, #, etc.).

"Private Information" refers to non-public personal, proprietary and confidential information, of Clients, the Agency and/or Agency employees.

"Systems" refers to all agency computers, networks, copiers, scanners, FAX machines, voice mail/phone systems, and other storage devices (e.g. back-up tapes, USB and other portable drives, CDs, etc.) where Agency Private Information might be found (whether maintained on Agency equipment/servers or on equipment/servers managed by third parties or employees, wherever located).

SCOPE & OBJECTIVE

This Plan for Agency is intended to create effective administrative, technical, electronic and physical protections to safeguard the personal information of the Agency's Clients and employees, the Agency's proprietary and confidential information, the physical security of our premises, and the integrity of our electronic systems so that they are best positioned to function smoothly without interruption.

This Plan sets forth the Agency's procedures for electronic and physical methods of accessing, collecting, storing, using, transmitting, destroying, and protecting Private Information of Clients, the Agency and/or Agency employees and also the use of the Agency's Systems by Agency employees and any authorized third parties, as deemed appropriate and/or required by applicable laws and regulations.

In formulating and implementing this Plan, we have:

(1) identified reasonably foreseeable internal and external risks to Agency's security, confidentiality and/or integrity of electronic, paper or other records containing Private Information;

(2) assessed the likelihood and potential danger of these threats, taking into consideration the sensitivity of the Private Information;

(3) evaluated the sufficiency of existing Agency policies, procedures, and other safeguards in place to minimize those risks;

(4) designed and implemented an approach that puts safeguards in place to minimize those risks, consistent with the requirements of applicable laws/regulations; and

(5) included regular monitoring of the effectiveness of those safeguards.

All security measures contained in this Plan shall be reviewed and re-evaluated annually or when there is a change in applicable laws or regulations or in the business activities of Agency. The Agency reserves the right to modify this Plan at any time, with or without prior notice.

EMPLOYEE RESPONSIBILITY

It shall be the responsibility of each Agency employee to carefully read, understand and adhere to this Plan. Each employee with access to Private Information shall receive training as necessary on this Plan and confirm in writing that he or she understands the requirements and will adhere to it as a continuing condition of his or her employment. Failure to adhere to the requirements of this Plan shall subject the employee to disciplinary action by Agency, up to and including termination.

OWNERSHIP OF AGENCY INFORMATION

The Agency regards all information contained, sent or received on the Agency's Systems and/or Agency equipment (e.g., Agency computers and mobile electronic devices, email, text and instant messaging systems, social networks and message boards, whether maintained on Agency equipment/servers or on equipment/servers managed by others) as well as information contained in, sent or received by Agency employees about the Agency or relating to its business on non-Agency equipment, as the property of the Agency, and the Agency reserves the right to access, review, use and disclose any such information at any time, with or without notice to employee, in Agency's sole discretion. Employees have no right to or expectation of privacy with respect to any such information (except for the Private Information relating specifically to them), and shall acquire no ownership or control rights over such information.

INFORMATION SECURITY OFFICER

The Agency has designated Shawn Haindel as the "Compliance Officer" to oversee implementation of this Plan.

The Compliance Officer will be responsible for:

1. Initial implementation of this Plan;
2. Training existing and new employees;
3. Appropriate testing and evaluation of this Plan's safeguards;
4. Evaluating the ability of service providers to comply with this Plan and applicable laws/regulations;
5. Reviewing the security measures in this Plan annually or when there is a change in applicable laws or regulations or in business activities of Agency; and
6. Conducting training as necessary for all Agency employees with access to Private Information.

SPECIAL PROTECTION FOR PRIVATE INFORMATION

Private Information is to be accorded the highest level of confidentiality by the Agency and employees.

Examples of Private Information include, but are not limited to

1. First name and last name, or first initial and last name, **and** any one or more of the following:
2. Social Security number;
3. Driver's license number, passport number, or state-issued identification card number;
4. Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password; and/or
5. Personal or protected health information.

The information listed in 2-5 above, even if it is not connected with a name, should each be treated as Private Information because of the potential for identity to be stolen from possession of just the numbers or information.

WHERE PRIVATE INFORMATION IS STORED

The Agency and its employees recognize that the Agency possesses Private Information in the following places, whether in the Agency's premises or off site, and whether created or maintained by Agency or third parties on behalf of Agency:

- hard copy and electronic files on Clients and employees, located at desks, in file drawers, storage areas and on the Agency's Systems;
- personnel files, Form I-9s, benefits information, payroll information, and direct deposit information for employees wherever located, including but not limited to hard copies at desks, in file drawers and other storage areas, and in electronic form on the Agency's Systems;
- off-site back-ups, in any form; and
- third-party vendors entrusted with Private Information from the Agency.

This Plan is intended to protect Private Information possessed by the Agency from unauthorized access, dissemination and/or use.

Private Information may not be disseminated, communicated or stored on or through any social media websites or services, at any time or for any reason.

INTERNAL RISKS TO PRIVATE INFORMATION & AGENCY SECURITY

To combat internal risks to the security, confidentiality and/or integrity of records containing Private Information, the following measures will be taken:

1. Agency employees will be given access to Private Information only for appropriate business purposes, as necessary, within their job duties. Access is granted through the User Set-Up Form as described in the employee handbook.
2. The Agency will encrypt and password-protect Private Information in its Systems to the extent reasonably practical, as determined by Agency management.
3. The Agency will retain only the last four digits of credit card numbers.

4. Paper documents containing Private Information will be placed in a file folder or put in a cabinet or drawer so Private Information is not accessible to others. When leaving for the day, all files and paperwork containing any confidential information should be locked up in either a file cabinet or drawer. Electronic files containing Private Information will not be left accessible to others. Paper and electronic files must not be accessed remotely unless specific authorization has been provided in advance, and then, the security of that Private Information must be maintained.

5. Employees are expected to log off or lock their computers when they leave the building or are away from their desk for an extended period of time.

   Agency computers will require a user ID and password. Employee log-ins and passwords should be appropriately strong (with the minimum number of characters and other elements required by the Agency's Systems). The Agency will remind all employees of the requirement to change their computer passwords every 90 days, and employees will only share their passwords with their immediate supervisor and/or system administrator. Passwords will be protected in a locked drawer or a password protected file. Electronic access to employee workstations will be blocked after multiple unsuccessful attempts to log-in.

   Employees should keep **all** mobile electronic communications devices with access to Private Information in their possession or in a secured location at all times, and Employees will not share passwords or other access information with others.

   Employees will not put any Agency data on thumb drives, laptops or other portable media, drives and devices unless authorized by the Agency. If so authorized, the thumb drives, laptops or other portable media, drives and devices must be password-protected and encrypted. All portable mobile electronic communications devices and laptops must be password-protected and encrypted.

6. Employees will adhere to the Agency document retention schedule and requirements. When it is appropriate to destroy Agency records, paper and electronic records containing Private Information must be destroyed in a manner in which Private Information cannot be read or reconstructed. Employees may shred their own materials in one of the copy rooms or they may utilize the locked shredding bins located in the recycling room. When computers, digital copiers, scanners and/or printers with electronic storage capacity, or portable electronic devices and media are discarded, such disposal should be coordinated with the information and technology coordinator, and care needs to be taken to ensure that the hard drives or other storage media are destroyed in a manner that all data becomes unreadable.

7. The communications and technology coordinator is responsible for terminating all of the employee's IDs and passwords to the Agency's Systems and invalidating the employee's access to Agency intranet and Agency-sponsored social media, immediately upon the employee's ceasing to work for the Agency or when directed by Agency management.

   The information and technology coordinator shall be notified immediately of any employee ceasing to work for the Agency, so that he or she can take immediate action to deactivate all passwords to which the former employee had access.

8. Employees that no longer work for the Agency must: (1) return to Agency all Agency information (including, but not limited to, any Private Information) in any form, whether

stored on computers, laptops, portable devices, electronic media, or in files, records, work papers, etc.; (2) return all keys, IDs, access codes and/or badges; and (3) not access non-public Agency information (including, but not limited to, any Private Information).

9. In accordance with the Agency's human resources manual, access by the former employee to Agency email and voice mail accounts can be immediately disabled and access transferred to other Agency staff to assure a continuity of work, and inactivated when determined appropriate by Agency.

10. Employees are required to report all actual or potential unauthorized access to, use of or disclosure of Private Information to the Information Security Officer.

EXTERNAL RISKS TO PRIVATE INFORMATION & AGENCY SECURITY

In addition to the measures taken to combat internal risks, the following measures will be taken to minimize external risks to the security, confidentiality and/or integrity of records containing Private Information:

1. Visitors to the Agency will be escorted within the office and will not have access to Agency computers or property that may contain Private Information. Guests' wireless access should be fire-walled off from the Agency's Systems.

2. The Agency will maintain security measures so that its wireless networks cannot be accessed remotely by the public.

3. During non-office hours, the Agency will be locked and have a central station-reporting security system activated.

4. Servers and other equipment at the Agency's premises containing Private Information will be maintained in a secure location.

5. Employees should not open any email attachment, link, or application where the employee does not reasonably believe the information expected to be accessed is from a trustworthy source. Employees will not use Agency equipment to access any application or software not approved by the Agency.

6. The Agency will employ an email filter (hardware, software, or third-party provided) that works to restrict and eliminate viruses, spyware and other malware before getting to Agency desktop and portable computers.

7. The Agency will maintain up-to-date network and firewall protection and operating system security patches on its Systems, servers and desktop and laptop computers, as well as other security measures deemed appropriate. The Agency will maintain security software, which includes malware protection with up-to-date patches and virus definitions, on its Systems and its servers, desktop and laptop computers, which is updated as frequently as possible, but at least daily.

8. All back-ups will be password-protected and encrypted and kept in a secured location off site.

9. Agency employees should use care in communications (e.g., outgoing email and attachments) to ensure: first, that the Private Information needs to be sent by email and, if so, that it is transmitted using secure email in accordance with Agency policy.

10. The Agency will create a secure SSL tunnel between its website and the consumer before allowing the consumer to enter any Private Information or to enter a password.

11. When an employee accesses Agency Systems and/or Private Information from a remote location, the Agency's secure SSL connection must be used (such as Virtual Private Network, GoToMyPC, LogMeIn). Private Information transmitted across public networks or wirelessly should always be encrypted.

12. Employees should not access Agency Systems or Private Information using non-Agency equipment (e.g., a home computer) unless authorized by the Agency and provided with appropriate firewalls and virus protection, and done through the Agency's secure SSL connection. Employees will not store any Private Information on any non-Agency equipment.

13. The Agency may monitor its Systems and equipment for unauthorized use, including but not limited to implementing hardware, software and/or procedural mechanisms to record and report activity for the Systems and equipment, without further notice to employees.

14. The Agency will exercise due diligence in making sure third-party vendors that are provided Private Information have the requisite security controls and written plan in place, provide the Agency a written commitment to safeguard and store Private Information with at least the same level of security controls as the Agency maintains (as outlined in this Plan), and advise the Agency as to any actual, suspected or potential breaches of Private Information.

IF A BREACH OF PRIVATE INFORMATION OCCURS OR IS SUSPECTED

A security breach occurs when there is an unauthorized acquisition, dissemination, use or loss of Private Information. Each employee shall be responsible for notifying the Compliance Officer whenever he or she learns that there has been or *may* have been a security breach that may have compromised Private Information or other Agency information about Clients, employees or Agency business.

The Agency will take the following actions in the event of a security breach:

a. assess the security breach;
b. consult counsel;
c. review the requirements of the applicable state laws and regulations;
d. notify the carriers whose policyholders insured through the Agency may have been affected by the event;
e. notify individuals, regulatory and law enforcement authorities (if and as required and further as deemed appropriate by Agency management);
f. take and document corrective actions to contain and control the problem;
g. identify who will address any media inquiries; and
h. draft the content of all communications regarding the event for potentially affected individuals and, if appropriate, the public.

By receipt of this Employee Handbook all employees acknowledge receipt of this Information Security Plan.
August 2019

MDA SPECIFIC - INFORMATION SECURITY PLAN

DEFINITIONS

Please carefully review the definition of these terms, because they are used frequently in this plan:

"Plan" refers to the Information Security Plan.

"Company" refers to the Michigan Dental Association (MDA)

"Members/Customers" refers to the MDA's members/customers, along with former and prospective members/customers.

"Encrypted" refers to the use of a program to put computer data into a coded format that cannot be read by unauthorized users.

"Passwords" refers to a string of characters that, when possible, is at least 8 characters long and contains at least three of the following: upper case letter, lower case letter, a number, a special character (%, &, #, etc.).

"Private Information" refers to non-public personal, proprietary and confidential information, of Clients, the Agency and/or Agency employees.

"Systems" refers to all MDA computers, networks, copiers, scanners, fax machines, voice mail/phone systems, and other storage devices (e.g. back-up tapes, USB and other portable drives, CDs, etc.) where company private Information might be found (whether maintained on company equipment/servers or on equipment/servers managed by third parties or employees, wherever located).

SCOPE & OBJECTIVE

This Plan for the Company is intended to create effective administrative, technical, electronic and physical protections to safeguard the personal information of the Company's Members/Customers and employees, the Company's proprietary and confidential information, the physical security of our premises, and the integrity of our electronic systems so that they are best positioned to function smoothly without interruption.

This Plan sets forth the Company's procedures for electronic and physical methods of accessing, collecting, storing, using, transmitting, destroying, and protecting Private Information of Members/Customers, the Company and/or Company employees and also the use of the Company's Systems by Company employees and any authorized third parties, as deemed appropriate and/or required by applicable laws and regulations.

In formulating and implementing this Plan, we have:

(1) identified reasonably foreseeable internal and external risks to Company's security, confidentiality and/or integrity of electronic, paper or other records containing Private Information;

(2) assessed the likelihood and potential danger of these threats, taking into consideration the sensitivity of the Private Information;

(3) evaluated the sufficiency of existing Company policies, procedures, and other safeguards in place to minimize those risks;

(4) designed and implemented an approach that puts safeguards in place to minimize those risks, consistent with the requirements of applicable laws/regulations; and

(5) included regular monitoring of the effectiveness of those safeguards.

All security measures contained in this Plan shall be reviewed and re-evaluated annually or when there is a change in applicable laws or regulations or in the business activities of Agency. The Company reserves the right to modify this Plan at any time, with or without prior notice.

EMPLOYEE RESPONSIBILITY

It shall be the responsibility of each Company employee to carefully read, understand and adhere to this Plan. Each employee with access to Private Information shall receive training as necessary on this Plan and confirm in writing that he or she understands the requirements and will adhere to it as a continuing condition of his or her employment. Failure to adhere to the requirements of this Plan shall subject the employee to disciplinary action by Company, up to and including termination.

OWNERSHIP OF AGENCY INFORMATION

The Company regards all information contained, sent or received on the Company's Systems and/or Company equipment (e.g., Company computers and mobile electronic devices, email, text and instant messaging systems, social networks and message boards, whether maintained on Company equipment/servers or on equipment/servers managed by others) as well as information contained in, sent or received by Company employees about the Company or relating to its business on non-Company equipment, as the property of the Company, and the Company reserves the right to access, review, use and disclose any such information at any time, with or without notice to employee, in Company's sole discretion. Employees have no right to or expectation of privacy with respect to any such information (except for the Private Information relating specifically to them), and shall acquire no ownership or control rights over such information.

INFORMATION SECURITY OFFICER

The Company has designated Shawn Haindel as the "Compliance Officer" to oversee implementation of this Plan.

The Compliance Officerwill be responsible for:

1. Initial implementation of this Plan;
2. Training existing and new employees;
3. Appropriate testing and evaluation of this Plan's safeguards;
4. Evaluating the ability of service providers to comply with this Plan and applicable laws/regulations;
5. Reviewing the security measures in this Plan annually or when there is a change in applicable laws or regulations or in business activities of Agency; and

6. Conducting training as necessary for all Company employees with access to Private Information.

SPECIAL PROTECTION FOR PRIVATE INFORMATION

Private Information is to be accorded the highest level of confidentiality by the Company and employees.

Examples of Private Information include, but are not limited to

1. First name and last name, or first initial and last name, **and** any one or more of the following:
2. Social Security number;
3. Driver's license number, passport number, or state-issued identification card number;
4. Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password; and/or
5. Personal or protected health information.

The information listed in 2-5 above, even if it is not connected with a name, should each be treated as Private Information because of the potential for identity to be stolen from possession of just the numbers or information.

WHERE PRIVATE INFORMATION IS STORED

The Company and its employees recognize that the Company possesses Private Information in the following places, whether in the Agency's premises or off site, and whether created or maintained by Agency or third parties on behalf of Agency:

- hard copy and electronic files on Members/Customers and employees, located at desks, in file drawers, storage areas and on the Company's Systems;
- personnel files, Form I-9s, benefits information, payroll information, and direct deposit information for employees wherever located, including but not limited to hard copies at desks, in file drawers and other storage areas, and in electronic form on the Company's Systems;
- off-site back-ups, in any form; and
- third-party vendors entrusted with Private Information from the Company.

This Plan is intended to protect Private Information possessed by the Company from unauthorized access, dissemination and/or use.

Private Information may not be disseminated, communicated or stored on or through any social media websites or services, at any time or for any reason.

INTERNAL RISKS TO PRIVATE INFORMATION & COMPANY SECURITY

To combat internal risks to the security, confidentiality and/or integrity of records containing Private Information, the following measures will be taken:

1. Agency employees will be given access to Private Information only for appropriate business purposes, as necessary, within their job duties. Access is granted through the User Set-Up Form as described in the employee handbook.

2. The Company will encrypt and password-protect Private Information in its Systems to the extent reasonably practical, as determined by Company management.

3. The Company will retain only the last four digits of credit card numbers.

4. Paper documents containing Private Information will be placed in a file folder or put in a cabinet or drawer so Private Information is not accessible to others. When leaving for the day, all files and paperwork containing any confidential information should be locked up in either a file cabinet or drawer. Electronic files containing Private Information will not be left accessible to others. Paper and electronic files must not be accessed remotely unless specific authorization has been provided in advance, and then, the security of that Private Information must be maintained.

5. Employees are expected to log off or lock their computers when they leave the building or are away from their desk for an extended period of time.

   Agency computers will require a user ID and password. Employee log-ins and passwords should be appropriately strong (with the minimum number of characters and other elements required by the Company's Systems). The Company will remind all employees of the requirement to change their computer passwords every 90 days, and employees will only share their passwords with their immediate supervisor and/or system administrator. Passwords will be protected in a locked drawer or a password protected file. Electronic access to employee workstations will be blocked after multiple unsuccessful attempts to log-in.

   Employees should keep mobile electronic communications devices (such as PDAs, Blackberries, smart phones, etc.) with access to Private Information in their possession or in a secured location at all times, and Employees will not share passwords or other access information with others.

   Employees will not put any Company data on thumb drives, laptops or other portable media, drives and devices unless authorized by the Company. If so authorized, the thumb drives, laptops or other portable media, drives and devices must be password-protected and encrypted. All portable mobile electronic communications devices and laptops must be password-protected and encrypted.

6. Employees will adhere to the Company document retention schedule and requirements. When it is appropriate to destroy Company records, paper and electronic records containing Private Information must be destroyed in a manner in which Private Information cannot be read or reconstructed. Employees may shred their own materials in one of the copy rooms or they may utilize the locked shredding bins located in the recycling room. When computers, digital copiers, scanners and/or printers with electronic storage capacity, or portable electronic devices and media are discarded, such disposal should be coordinated with the information and technology coordinator, and care needs to be taken to ensure that the hard drives or other storage media are destroyed in a manner that all data becomes unreadable.

7. The communications and technology coordinator is responsible for terminating all of the employee's IDs and passwords to the Company's Systems and invalidating the employee's access to Company intranet and Company-sponsored social media, immediately upon the employee's ceasing to work for the Agency or when directed by Company management.

The communications and technology coordinator shall be notified immediately of any employee ceasing to work for the Company, so that he or she can take immediate action to deactivate all passwords to which the former employee had access.

8. Employees that no longer work for the Company must: (1) return to Company all Company information (including, but not limited to, any Private Information) in any form, whether stored on computers, laptops, portable devices, electronic media, or in files, records, work papers, etc.; (2) return all keys, IDs, access codes and/or badges; and (3) not access non-public Company information (including, but not limited to, any Private Information).

9. In accordance with the Company's human resources manual, access by the former employee to Company email and voice mail accounts can be immediately disabled and access transferred to other Company staff to assure a continuity of work, and inactivated when determined appropriate by Company.

10. Employees are required to report all actual or potential unauthorized access to, use of or disclosure of Private Information to the Information Security Officer.

EXTERNAL RISKS TO PRIVATE INFORMATION & AGENCY SECURITY

In addition to the measures taken to combat internal risks, the following measures will be taken to minimize external risks to the security, confidentiality and/or integrity of records containing Private Information:

1. Visitors to the Company will be escorted within the office and will not have access to Company computers or property that may contain Private Information. Guests' wireless access should be fire-walled off from the Company's Systems.

2. The Company will maintain security measures so that its wireless networks cannot be accessed remotely by the public.

3. During non-office hours, the Company will be locked and have a central station-reporting security system activated.

4. Servers and other equipment at the Company's premises containing Private Information will be maintained in a secure location.

5. Employees should not open any email attachment, link, or application where the employee does not reasonably believe the information expected to be accessed is from a trustworthy source. Employees will not use Company equipment to access any application or software not approved by the Company.

6. The Company will employ an email filter (hardware, software, or third-party provided) that works to restrict and eliminate viruses, spyware and other malware before getting to Company desktop and portable computers.

7. The Company will maintain up-to-date network and firewall protection and operating system security patches on its Systems, servers and desktop and laptop computers, as well as other security measures deemed appropriate. The Company will maintain security software, which includes malware protection with up-to-date patches and virus definitions,

on its Systems and its servers, desktop and laptop computers, which is updated as frequently as possible, but at least daily.

8. All back-ups will be password-protected and encrypted and kept in a secured location off site.

9. Company employees should use care in communications (e.g., outgoing email and attachments) to ensure: first, that the Private Information needs to be sent by email and, if so, that it is transmitted using secure email in accordance with Company policy.

10. The Company will create a secure SSL tunnel between its website and the consumer before allowing the consumer to enter any Private Information or to enter a password.

11. When an employee accesses Company Systems and/or Private Information from a remote location, the Company's secure SSL connection must be used (such as Virtual Private Network, GoToMyPC, LogMeIn). Private Information transmitted across public networks or wirelessly should always be encrypted.

12. Employees should not access Company Systems or Private Information using non-Company equipment (e.g., a home computer) unless authorized by the Company and provided with appropriate firewalls and virus protection, and done through the Agency's secure SSL connection. Employees will not store any Private Information on any non-Company equipment.

13. The Company may monitor its Systems and equipment for unauthorized use, including but not limited to implementing hardware, software and/or procedural mechanisms to record and report activity for the Systems and equipment, without further notice to employees.

14. The Company will exercise due diligence in making sure third-party vendors that are provided Private Information have the requisite security controls and written plan in place, provide the Company a written commitment to safeguard and store Private Information with at least the same level of security controls as the Company maintains (as outlined in this Plan), and advise the Company as to any actual, suspected or potential breaches of Private Information.

IF A BREACH OF PRIVATE INFORMATION OCCURS OR IS SUSPECTED

A security breach occurs when there is an unauthorized acquisition, dissemination, use or loss of Private Information. Each employee shall be responsible for notifying the Compliance Officerwhenever he or she learns that there has been or *may* have been a security breach that may have compromised Private Information or other Company information about Members/Customers, employees or Company business.

The Company will take the following actions in the event of a security breach:

a. assess the security breach;
b. consult counsel;
c. review the requirements of the applicable state laws and regulations;
d. notify the carriers whose policyholders insured through the Company may have been affected by the event;
e. notify individuals, regulatory and law enforcement authorities (if and as required and further as deemed appropriate by Company management);
f. take and document corrective actions to contain and control the problem;

g. identify who will address any media inquiries; and
h. draft the content of all communications regarding the event for potentially affected individuals and, if appropriate, the public.

By receipt of this Employee Handbook all employees acknowledge receipt of this Information Security Plan.

IFG - HIPAA PRIVACY PRACTICES PROTOCOL

This Protocol is amended and restated effective February 17, 2010 to provide guidance to MDA Insurance and Financial Group, Inc. ("MDA IFG") so that it acts in a manner consistent with the responsibilities of a business associate of a health plan ("Health Plan") under the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations including the Privacy Rule (codified at 45 C.F.R. Parts 160 and 164, subparts A and E) and the Security Rule (codified at 45 C.F. R. Parts 160 and 164, subparts A and C) (Collectively "HIPAA"), and the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 and regulations promulgated thereunder by the U.S. Department of Health and Human Services ("the HITECH Act"). This Protocol applies only to the extent that MDA IFG functions as a business associate of a Health Plan. This Protocol is intended for internal use by MDA IFG and its employees and may be amended, repealed or superseded at any time by MDA IFG in its discretion. To the extent that MDA IFG and a Health Plan have contractually agreed to standards which are more stringent than, or in addition to, those set forth in this Protocol, the more stringent standards, and any additional standards, shall apply and shall supersede the standards set forth in this Protocol.

1. **Protected Health Information.** The term "Protected Health Information" shall have the meaning defined at 45 CFR §164.501 and shall refer to Protected Health Information which MDA IFG receives, uses and discloses in so far as it functions as a business associate of a Health Plan.

2. **Permitted Uses and Disclosures.** MDA IFG may receive, use and disclose Protected Health Information for the purpose of functioning as a business associate of a Health Plan. These functions include, but are not necessarily limited to, ensuring that Health Plan enrollees submit completed applications (which may contain health history and other Protected Health Information), forwarding applications to Health Plans, and storing applications. MDA IFG may use and disclose Protected Health Information for MDA IFG's proper management and administration or to carry out MDA IFG's legal responsibilities, but only in conformity with HIPAA, the HITECH Act and this Protocol. Any use or disclosure of Protected Health Information will be only to the minimum extent necessary to accomplish the purpose of the use or disclosure.

3. **Prohibition on Unauthorized Use or Disclosure.** MDA IFG will neither knowingly use nor disclose Protected Health Information to persons other than a Health Plan (including a sponsoring employer), except as permitted or required by HIPAA, the HITECH Act, or other law, or as otherwise permitted in writing by a Health Plan or by a Health Plan enrollee's written authorization. MDA IFG shall not use or disclose Protected Information for fundraising or marketing purposes. MDA IFG shall not disclose Protected Health Information to a Health Plan for payment or health care operations purposes if the patient has requested this special restriction, and has paid out of pocket in full for the health care item or service to which the Protected Health Information solely relates in accordance with 42 U.S.C. Section 17935(a). MDA IFG shall not directly or indirectly receive remuneration in exchange for Protected Health Information, except with the prior written consent of the Health Plan and as permitted by the HITECH Act, 42 U.S.C. Section 17935(d)(2); however, this prohibition shall not affect payment by the Health Plan to MDA IFG for services provided pursuant to the contract.