HIPAA PRIVACY PRACTICES PROTOCOL

4-3510 **RESOLVED**, that the MDA Insurance & Financial Group Board of Directors adopt the HIPAA Privacy Practices Protocol dated February 17, 2010.

This protocol is amended and restated effective February 17, 2010 to provide guidance to MDA Insurance & Financial Group, Inc. ("MDAIFG") 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 MDAIFG functions as a business associate of a Health Plan. This Protocol is intended for internal use by MDAIFG and its employees and may be amended, repealed or superseded at any time by MDAIFG in its discretion. To the extent that MDAIFG 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 MDAIFG receives, uses and discloses insofar as it functions as a business associate of a Health Plan.

2. Permitted Uses and Disclosures. MDAIFG 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. MDAIFG may use and disclose Protected Health Information for MDAIFG's proper management and administration or to carry out MDAIFG'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. MDAIFG 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. MDAIFG shall not use or disclose Protected Information for fundraising or marketing purposes. MDAIFG 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. § 17935(a). MDAIFG 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 MDAIFG for services provided pursuant to the contract.

4. Disclosure to Subcontractors and Agents. If it is necessary for MDAIFG to disclose Protected Health Information to any of its subcontractors or agents for a purpose permitted by HIPAA and the HITECH Act, MDAIFG will first require such persons to agree in writing to assume the responsibilities of a HIPAA business associate.

5. Information Safeguards. MDAIFG will use reasonable and appropriate administrative, technical and physical safeguards to preserve the integrity and confidentiality of, and to prevent non-permitted uses or disclosures of, Protected Health Information, in accordance with 45 C.F.R. § 164.308, 164.310, and 164.312. MDAIFG shall comply with the policies and procedures and documentation requirements of the HIPAA Security Rule, including, but not limited to, 45 C.F.R. § 164.316. Any access to Protected Health Information by MDAIFG employees or subcontractors/agents will be on a need to know basis, and only then to the minimum extent necessary for the person to carry out the designated function.

6. Access. To the extent required by HIPAA and the HITECH Act, MDAIFG, on reasonable advance written notice, will make available to a Health Plan for inspection and copying (at the Health Plan's cost) any Protected Health Information in MDAIFG's custody or control, so that the Health Plan may meet its access obligations under HIPAA and the HITECH Act. MDAIFG does not maintain an Electronic Health Record (as such term is defined in the HITECH Act, including, but not limited to, 42 U.S.C. Section 17921).

7. Amendment. To the extent required by HIPAA and the HITECH Act, MDAIFG will, upon receipt of written notice from a Health Plan, promptly amend, or permit the Health Plan access to amend, any portion of the Protected Health Information in MDAIFG's custody or control, so that the Health Plan may meet its amendment obligations under HIPAA and the HITECH Act.

8. Disclosure Accounting. To the extent required by HIPAA and the HITECH Act, MDAIFG will record for each disclosure of Protected Health Information, not excepted from HIPAA's disclosure accounting standards, such information as required by HIPAA, so that a Health Plan may meet its disclosure accounting obligations under HIPAA and the HITECH Act, including but not limited to 42 U.S.C. Section 17935(c).

9. Inspection of Books and Records. To the extent required by HIPAA and the HITECH Act, MDAIFG will make its internal practices, books and records, relating to its

use and disclosure of the Protected Health Information on behalf of a Health Plan, available for inspection by the Health Plan and the U.S. Department of Health and Human Services to assess compliance with applicable standards under HIPAA and the HITECH Act.

10. Reporting. MDAIFG will timely report to a Health Plan any known use, access or disclosure of Protected Health Information not permitted by this Protocol or HIPAA and the HITECH Act and any Breach of Unsecured PHI of which it becomes aware without unreasonable delay and in no case later than five (5) business days after discovery. "Breach" shall have the meaning given to such term under the HITECH Act, 42 U.S.C. Section 17921. "Unsecured PHI" shall have the meaning given to such term under the HITECH Act and any guidance issued pursuant to such Act including, but not limited to, 42 U.S.C. Section 17932(h).

11. Breach Pattern or Practice by Health Plan. Pursuant to 42 U.S.C. Section 17934(b), if the MDAIFG knows of a pattern of activity or practice of the Health Plan that constitutes a material breach or violation of the Health Plan's obligations under the contract or Addendum or other arrangement, the Health Plan must take reasonable steps to cure the breach or end the violation. If the steps are unsuccessful, MDAIFG must terminate the contract or other arrangement if feasible, or if termination is not feasible, report the problem to the Secretary of DHHS.

12. Responsibilities Following Termination of Health Plan Relationship. The responsibilities of MDA IFG under this Protocol are continuous and shall survive any termination of any business associate relationship between MDAIFG and a Health Plan. If and when a business associate relationship ceases, the retention, or destruction of Protected Health Information shall be dealt with in the manner to be determined by MDAIFG and the Health Plan, subject to the requirements of HIPAA and the HITECH Act.

13. Measures to Promote Compliance. In an effort to assess and promote compliance with this Protocol, MDAIFG will:

- Designate, and document the designation of, an employee (the "Privacy Officer") who is responsible to oversee the implementation of this Protocol and the promotion of compliance.
- The Privacy Officer will train, and document the training of, affected MDAIFG employees regarding this Protocol and compliance. Training will be furnished to affected new employees within a reasonable time after beginning work.

- The Privacy Officer will assess whether MDAIFG has in place reasonable and appropriate administrative, technical and physical safeguards to maintain the confidentiality of, and to prevent non-permitted uses or disclosures of, Protected Health Information. For example, the Privacy Officer will assess whether

documents containing Protected Health Information, such as Health Plan enrollment applications, are stored in a secure manner, whether any computers maintaining Protected Health Information are adequately protected from unauthorized access, etc. The Privacy Officer will document and retain

the results of the assessment and of any modifications made to MDAIFG's business practices to promote compliance.

- MDAIFG will apply and document appropriate sanctions against employees who violate this Protocol.

- MDAIFG employees will be instructed to promptly report to the Privacy Officer any disclosure or use of Protected Health Information which violates this Protocol.

- MDAIFG will, as necessary from time to time, adopt and document reasonable policies, procedures and measures taken to promote compliance with HIPAA's business associate standards and the HITECH Act.

- MDAIFG will retain all documentation regarding compliance with this Protocol for a minimum of six years after the date the information was created or was last in effect.