

## ACA COMPLIANCE GROUP

### WRITTEN INFORMATION SECURITY PLAN (“WISP”)

Effective March 1, 2010

#### Summary

ACA Compliance Group (“ACA”) has developed and implemented a written information security plan (“WISP”) to establish effective safeguards to protect the personal and confidential information of its clients, employees, and other persons. This is a summary of ACA’s WISP.

ACA’s WISP is intended to ensure that ACA has a robust information safeguarding program. In addition, it addresses ACA’s obligations under Massachusetts information safeguarding law, 201 CMR 17. Specifically, ACA’s WISP is designed to:

- ensure the security and confidentiality of information received by, stored at, sent out, or otherwise used by ACA;
- protect against anticipated threats or hazards to the security or integrity of such information; and
- protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

The policies and procedures in ACA’s WISP broadly apply to all information, in paper or electronic form, and generally apply without regard to whether a particular document or record contains “Personal Information,” as defined in accordance with 201 CMR 17. However, in certain instances, specific procedures are required when a record or communication involves Personal Information (without regard to state residency of the individual).

All ACA employees are subject to the WISP. All ACA independent contractors are subject to the WISP at all times while performing services for ACA, except for the *ACA Insight* editor (who operates independently from ACA).

ACA’s General Counsel and ACA’s IT Manager serve as the “WISP Coordinators.” In developing and implementing the WISP, the WISP Coordinators:

- identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of electronic, paper or other records collected, maintained, sent, or used by ACA that contain personal or other sensitive information;
- assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of that information;

- evaluated the sufficiency of existing policies, procedures, information systems, and other safeguards in place to control risks; and
- designed and implemented the WISP in order to memorialize existing safeguards and establish new safeguards to minimize those risks.

On an ongoing basis, the WISP Coordinators are responsible for:

- implementing the WISP;
- training ACA staff on the WISP requirements;
- testing the WISP's safeguards;
- evaluating third party service providers to confirm that such service providers have established appropriate Personal Information protective security measures;
- reviewing the WISP at least annually, or whenever there is a material change in ACA's business practices that may implicate the security or integrity of records containing Personal Information or other sensitive information, or whenever there is an actual or threatened security breach event;
- reporting any material findings from any WISP review, and any material recommendations for improving the WISP arising out of such a review, to ACA's Management Committee.

The WISP describes a number of technology-based information security measures, safeguards, and procedures, covering the following areas:

- Network security;
- Laptop security;
- BlackBerry security;
- E-mail security;
- USB flashdrive (thumbdrive) security;
- CD-ROM/DVD security;
- Password security; and
- Firewalls, anti-virus protection, and malware protections.

The WISP addresses physical office security (locks/keys, desk policy, printers, faxes, visitor access, etc.). It contains special procedures from working in out of the office (i.e., in client offices, home offices, or in other public settings). It also sets forth procedures for training new ACA staff, processing departing employees, and disciplining ACA staff for WISP violations.

All ACA staff are required to certify that they have received a copy of the WISP, have read it, and intend to comply with its terms.

Additional questions about ACA's WISP should be directed to ACA's General Counsel, Cathie Saadeh, at (202) 955-5800.