

Bacon Wilson, P.C.
Comprehensive Written Information Security Program

I. Objective

The objective of this Comprehensive Written Information Security Program (“WISP”) is to establish effective protection of the Personal Information of residents of the Commonwealth of Massachusetts and to comply with our obligations under M.G.L. c. 93H, 93I, and 201 CMR 17.00. The electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting Personal Information set forth herein contain administrative, technical, and physical safeguards to ensure the security and confidentiality of such records, and are intended to be consistent with industry standards and any applicable state or federal regulations.

II. Goal

The goal of the WISP is to establish safeguards that:

- a) ensure the security and confidentiality of Personal Information;
- b) protect against anticipated threats or hazards to the security or integrity of such information; and
- c) protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

III. Definitions

The following words as used herein shall, unless the context requires otherwise have the following meanings pursuant to 201 CMR 17.00:

- a) “Breach of security” or “security breach,” the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of Personal Information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the Commonwealth. A good faith but unauthorized acquisition of Personal Information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the Personal Information is used in an unauthorized manner or subject to further unauthorized disclosure.
- b) “Electronic,” relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.
- c) “Encrypted,” the transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key, unless further regulated by the OCABR.
- d) “Firm Member” or “Firm Members,” any one or all of the group containing firm attorneys, full time, part time, temporary and contract employees and independent contractors.
- e) “OCABR,” the Office of Consumer Affairs and Business Regulation of the Commonwealth of Massachusetts.
- f) “Personal Information,” a Massachusetts resident’s last name in combination with: (1) that resident’s first name or first initial; and (2) the resident’s social security number, driver’s license number, state-issued identification number, financial account number, credit card number, or debit card number. Provided, however, that “Personal Information” shall not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

- g) "Record" or "Records," any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.
- h) "WISP Coordinator" or "WISP Coordinators," the individuals, or their assigns or successors, responsible for the implementation, maintenance, scope, and review of this WISP.

IV. WISP Coordinators

The WISP Coordinators shall work in unison to implement, supervise and maintain the WISP, shall review its safeguards at least annually or whenever there has been a material change in business practices or environment that may affect the security or integrity of records containing Personal Information, and shall have additional specific responsibilities designated as follows:

- a) Paul H. Rothschild and Jeffery I. Fialky shall:
 - 1. oversee the implementation of WISP and assure it maintains legal compliance with M.G.L. c. 93H, 93I, and 201 CMR 17.00 and any other applicable state and federal regulations;
 - 2. evaluate the ability of service providers to comply with 201 CMR 17.00 and other applicable regulations; and,
 - 3. ensure that all contracts with third-party service providers established after 03/01/2010 contain a provision obligating them to comply with 201 CMR 17.00 as required by that regulation.
- b) The Systems Administrator shall:
 - 1. be responsible for the implementation and maintenance of the WISP with respect to all electronic and computer related aspects; and,
 - 2. control access to the firm's network and perform regular tests of the network to ensure its security.
- c) The Executive Director, Executive Assistant and Accounting Administrator shall:
 - 1. be responsible for providing both initial and annual refresher training to and obtaining written confirmation of such training from all Firm Members on the WISP;
 - 2. control access to the Personal Information of current and former employees and clients;
 - 3. perform regular tests of established safeguards to ensure the security of such information; and,
 - 4. enforce the WISP as a term of employment and prescribe appropriate disciplinary measures for employees found in violation.

V. Safeguards

The following safeguards are intended to combat risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Personal Information, and to evaluate and improve where necessary their effectiveness in limiting or eliminating such risks.

- a) All Firm Members shall:
 - 1. in writing, acknowledge and agree to abide by the safeguards herein which shall be established in their initial/annual refresher training;
 - 2. remove Personal Information from plain view on their desk when they are not there;
 - 3. limit the amount of Personal Information collected to only that which is necessary to perform their job;
 - 4. dispose of unneeded documents containing any Personal Information in one of the clearly marked shred bins for shredding pursuant to M.G.L. c. 93I;

5. follow firm guidelines for closing inactive matters to ensure matter files are sent to our secure storage facility;
 6. check in and out with the Reception Desk upon entering and exiting the firm premises respectively;
 7. notify one of the WISP coordinators whenever they notice suspicious or unauthorized use of Personal Information and/or suspect there has been a breach of security;
 8. avoid faxing documents with Personal Information; or if unavoidable, be absolutely sure the recipient's fax number is correct, and if possible, black out the Personal Information;
 9. NOT take documents or files containing Personal Information outside the office unless required by duty (i.e., to Court), and if possible should black out any Personal Information;
 10. NOT share or write down their username, passwords or other user identifications;
 11. NOT send emails containing Personal Information unless such email is sent using the firm's encryption software in compliance with 201 CMR 17.00; and,
 12. NOT download or utilize any software, except for that approved and installed by the firm's Technology Services Department on firm personal computer or laptop systems.
- b) Terminated Employees shall:
1. return all records, in any form, that may be in their possession at the time of termination;
 2. immediately surrender all keys, IDs, access codes, badges, business cards, and the like, that permit access to the firm's premises and network;
 3. immediately surrender all property including laptops, cellular phones, PDAs, portable electronic and/or storage devices and any other electronic device belonging to the firm;

Upon termination, access to physical and electronic records and the firm's network will be terminated, and access to the premises will be strictly limited to that of non-employee visitors.

- c) Network Security shall be controlled by the Systems Administrator using the following safeguards:
1. every computer system that contains or processes Personal Information shall be installed with reasonably up-to-date firewall protection, system security agent software, including malware protection, operating system security and other patches, and virus definitions that are designed to maintain the integrity of Personal Information;
 2. secure user authentication protocols shall be established by the Systems Administrator including control over user accounts, requiring creation of strong passwords which include combinations of letters, numbers and special characters, and protecting the security of administrative network passwords;
 3. the network shall be monitored for unauthorized use or access;
 4. access to the network shall be restricted to only those Firm Members who require it to perform their duties;
 5. any account experiencing multiple unsuccessful attempts to gain access shall be automatically locked out after such attempts;
 6. to the extent technically feasible, all Personal Information stored on laptops or other portable devices and/or transmitted across public networks or wirelessly shall be encrypted.

- d) All Firm Members' Personal Information shall be maintained in securely locked cabinets in protected areas of the premises at all times, and access to such information shall be strictly controlled by the Executive Director and/or the Accounting Administrator to only those who must have access to such information for necessary administrative and/or accounting purposes.
- e) Clients' Personal Information shall be acquired with care and limited to only that which is absolutely necessary to provide proper legal services and/or for the Accounting Department to perform their duties; all Firm Members shall follow established safeguards to assure this information is secure.
- f) Visitors' access to the premises shall be restricted to the front door only; all visitors must register with the Reception Desk upon entering and leaving the premises and shall be escorted by a Firm Member at all times while on the premises.
- g) Inactive/Closed Matter Files shall be sent to a secure, locked storage facility that complies with 201 CMR 17.00 and other applicable regulations, presently New England Archives, and after a period of ten (10) years the entire file and its contents shall be destroyed by incineration or shredding pursuant to M.G.L. c. 93I.
- h) Third-Party Service Providers with access to Personal Information must provide written certification of their established information security policy and such policy must be in compliance with all applicable state and federal regulations. All contracts with third-party service providers entered into after 03/01/2010 shall include a term requiring such policy to be in place and for the provision of proof of same. Failure of any third-party service provider to satisfy the requirements of any applicable state or federal regulation regarding information security shall be grounds for breach of contract.

VI. Documentation and Notification

When an incident involving a breach of security occurs, the WISP Coordinator shall document any and all responsive actions taken in connection therewith and shall conduct a mandatory post-incident review of events and actions taken to prohibit future breaches. The WISP Coordinator shall notify the following individuals and entities in accordance with M.G.L. c. 93H:

- (1) All other firm WISP Coordinators;
- (2) The resident to whom the Personal Information belonged;
- (3) The Attorney General of the Commonwealth of Massachusetts; and
- (4) The Director of the OCABR.