

New York Addendum

Note: In addition to complying with federal identity theft prevention regulations, medical practices are required to comply with New York State consumer protection laws. These laws include criminal statutes that define identity theft and the unlawful possession of personal information as well as laws that define how to safeguard Social Security Numbers and explain what to do in the event of an inadvertent unauthorized disclosure. The following should, where applicable, be included in your identity theft prevention program:

In order to comply with The New York Social Security Number Protection Law (N.Y. Gen. Bus. Law § 399-dd) our Practice will not do the following with regard to a social security account number¹:

1. Intentionally communicate to the general public or otherwise make available to the general public in any manner an individual's social security account number;
2. Print an individual's social security account number on any card or tag required for the individual to access products, services or benefits provided by our Practice;
3. Require an individual to transmit his or her social security account number over the internet, unless the connection is secure or the social security account number is encrypted;
4. Require an individual to use his or her social security account number to access an internet web site, unless a password or unique personal identification number or other authentication device is also required to access the internet website.
5. Print an individual's social security account number on any materials that are mailed to the individual, unless state or federal law requires the social security account number to be on the document to be mailed. Notwithstanding this paragraph, social security account numbers may be included in applications and forms sent by mail, including documents sent as part of an application or enrollment process, or to establish, amend or terminate an account, contract or policy, or to confirm the accuracy of the social security account number. A social security account number that is permitted to be mailed under this section may not be printed, in whole or part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened.

¹ “Social security account number” shall include the number issued by the federal social security administration and any number derived from such number but not any number that has been encrypted.

6. Encode or embed a social security number in or on a card or document, including, but not limited to, using a bar code, chip, magnetic strip, or other technology, in place of removing the social security number as required by this section.
7. File any document available for public inspection with any state agency, political subdivision, or in any court of this state that contains a social security account number of any other person, unless such other person is a dependent child, or has consented to such filing, except as required by federal or state law or regulation, or by court rule.

This does not prevent our Practice's collection, use, or release of a social security account number as required by state or federal law, the use of a social security account number for internal verification, fraud investigation or administrative purposes or for any business function specifically authorized by law.

Our Practice will take reasonable measures to ensure that no employee has access to a social security number for any purpose other than for a legitimate or necessary purpose related to the conduct of our Practice and will provide safeguards necessary or appropriate to preclude unauthorized access to the social security account number and to protect the confidentiality of such number.

In order to comply with The New York State General Business Law § 899-aa, which outlines how our Practice should respond in the event of the breach of security of our computerized data system, our Practice will:

1. Disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York State whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made as provided in paragraph 4, below, in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system;
2. Notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization;
3. Potentially delay any necessary notification if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required shall be made after such law enforcement agency determines that such notification does not compromise such investigation;
4. Directly provide any required notice to the affected persons by one of the following methods:
 - (a) written notice;

- (b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by our Practice in such form; provided further, however, that in no case shall our Practice require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction with our Practice;
 - (c) telephone notification provided that a log of each such notification is kept by our Practice; or
 - (d) substitute notice after demonstrating to the state attorney general the necessary requirements;
5. Ensure that any required notice shall include contact information for our Practice and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired; and
6. Ensure that:
- (a) In the event that any New York residents are to be notified, the Practice shall notify the state attorney general, the consumer protection board, and the state office of cyber security and critical infrastructure coordination as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents; and that
 - (b) In the event that more than five thousand New York residents are to be notified at one time, the Practice shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.