Norris McLaughlin & Marcus, P.A.
ATTORNEYS AT LAW

NEW JERSEY DATA BREACH AND INFORMATION SECURITY NOTIFICATION POLICY

DISCLAIMER

This document is provided solely for informational purposes and to assist the typical physician practice which must undertake reasonable measures to comply with HIPAA Rules. While the document has been drafted to provide accurate and authoritative assistance, it is not intended as, and does not constitute legal or other professional advice, which can be rendered only on an individual practice and fact-sensitive basis. The information in it is not guaranteed to be correct, complete or up-to-date. Each practice must review this document for individualized adaptation to your practice or to a particular transaction. Readers should not act or elect not to act based upon the provided information without seeking professional legal advice from healthcare counsel.

NEW JERSEY DATA BREACH AND INFORMATION SECURITY NOTIFICATION POLICY

Purpose: To facilitate compliance with the requirements of the HITECH Act's Data Breach Notification Rule, and applicable New Jersey state law.

Definitions: The definitions attached hereto apply to this policy. Any terms not defined in the attachment shall have the meaning given them in the HIPAA Privacy Standards, 45 CFR Parts 160 and 164, as may be amended, or given them in the New Jersey Policy Addendum, attached hereto.

Policy: In the case of a breach of unsecured PHI, and as determined necessary pursuant to this policy, our Practice will provide the notifications as required herein. When such breach constitutes a "Breach of Security" under New Jersey law, our Practice will also comply with the attached New Jersey Policy Addendum. Our Practice will also comply with the restrictions on communication of Social Security Numbers, as set forth in the New Jersey Policy Addendum.

Procedures:

1. Discovery of Breach

    a. A breach is considered discovered as of the first day on which the breach is known by the Practice or, by exercising reasonable diligence, would have been known to the Practice.

    b. The Practice is deemed to have knowledge of a breach if the breach is known or, by exercising reasonable diligence, would have been known, to any person (other than the person committing the breach) who is an employee, officer or agent of the Practice. We do not consider a Business Associate to be an agent of the Practice but this is a fact-specific determination based on how much control we have over the Business Associate's performance of services on our behalf.

    c. Every member of our workforce (including owners, employees, contractors, volunteers, and trainees) shall immediately report to our Privacy Officer any information regarding a security incident, or a potential breach of PHI.

2. Investigation of Security Incident

    a. Our Privacy Officer shall be primarily responsible for investigating a security incident and will consult with our managing physician and our legal counsel in conducting such investigation. The investigation shall be conducted as promptly and expeditiously as possible, while addressing and documenting each step of the investigation.

    b. The first step in the investigation shall be to determine if the PHI involved was secured or unsecured PHI. (See Definitions accompanying this policy.) If the PHI was unsecured, the Privacy Officer shall continue to the second step. If the PHI was secured, no breach notification is required, but the Practice will take reasonably necessary steps to mitigate

any harm, impose required sanctions, and to assess and implement needed measures to avoid future security incidents of the same nature.

c. The second step in the investigation shall be to determine if the acquisition, access, use or disclosure of PHI was a violation of the Privacy Rule and, thus, impermissible, or if an exception applies. (See definition of breach.) If there was a violation of the Privacy Rule, and no exception applies, our Privacy Officer shall continue to the third step.

d. The third step in the investigation shall be to conduct a risk assessment to determine if the impermissible acquisition, access, use or disclosure of PHI compromises the security or privacy of the PHI. The impermissible acquisition, access, use or disclosure of PHI is presumed to be a breach, requiring notification, unless our Practice can demonstrate that there is a low probability that the PHI has been compromised, based on a risk assessment of at least the following factors:

    i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

    ii. The unauthorized person who used the PHI or to whom the disclosure was made;

    iii. Whether the PHI was actually acquired or viewed; and

    iv. The extent to which the risk to the PHI has been mitigated.

e. Our Privacy Officer shall consult with the managing physician and legal counsel in conducting the required risk assessment and making a determination as to whether the impermissible acquisition, access, use or disclosure of PHI constituted a breach that requires notification. If the determination is made that notification is required, our Privacy Officer shall implement the notification procedures required by this policy.

f. Concurrent with the steps taken above, our Practice will determine if the security incident involved computerized data involving Private Information and, if so, our Practice will incorporate the procedures contained in the New York Policy Addendum, including any notification procedures.

3. Notification Procedures

a. Timeliness of Notification

    i. Once a determination has been made that a breach notification is required, notice of the breach shall be made promptly to the patient(s) who we know, or reasonably believe, to be affected, without unreasonable delay, and in no case later than sixty (60) days after discovery of the breach. Note: The investigation conducted pursuant to Section 2 of this Policy does not stop the 60 day period from continuing to run from the date the breach was first discovered.

ii. Delay of Notice for Law Enforcement Purposes – If a law enforcement official advises our Practice that a notification, notice or posting required under this policy would impede a criminal investigation or cause damage to national security, our Practice shall take the following steps:

- If the statement is in writing and specifies the time needed for delay, our Practice shall delay breach notification for the period of time specified in the writing

- If the statement is oral, our Practice will document the statement, including the identity of the law enforcement official, and shall delay breach notification temporarily, but no longer than 30 days from the date of the statement, unless a written statement described above is provided to the Practice within that 30-day time period, stating a specific time for delay.

b. Content of the Notice – Regardless of the method by which notice is provided to patients under this policy, the required notice shall be in plain language and, to the extent possible, shall contain the following information:

i. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

ii. A description of the types of unsecured PHI that were involved in the breach, such as whether full name, Social Security Number, date of birth, home address, account number, diagnosis code, or disability code, or other types of information were involved. Only the generic type of PHI should be included in the notice, i.e., not the patient's actual SSN or birth date.

iii. The steps the patient should take to protect themselves from potential harm resulting from the breach.

iv. A brief description of what the Practice is doing to investigate the breach, to mitigate harm to patients, and to protect against further breaches.

v. Contact procedures for patients to ask questions or learn additional information, which shall include a toll-free telephone number, an email address, Web site, or postal address.

c. Patient Notification – Notice to individual patients shall be provided as follows:

i. A written notice shall be sent by first-class mail to the last known address of the patient or, if the patient has previously agreed to electronic notice, then by electronic mail (preferably encrypted).

ii. If the Practice knows that the patient is deceased, the notice shall be sent to the last known address of the patient's next of kin, if known to the Practice.

iii. If the patient is incapacitated or incompetent, the notice shall be sent to the last known address of the patient's personal representative.

iv. If the patient is a minor, the notice shall be sent to the last known address of the patient's parent or guardian.

d. Substitute Notification – In the case where there is insufficient or out-of-date contact information (including a phone number, email address or other form of appropriate communication) to provide direct written notice to the patient, the following procedure shall be followed:

i. If there are fewer than ten (10) patients for whom there is out-of-date or insufficient contact information, a substitute form of notice shall be made to the patient reasonably calculated to reach the patient, such as telephone contact, followed by written notice, if possible.

ii. If there are ten (10) or more patients for whom there is out-of-date or insufficient contact information, the substitute form of notice shall be made by:

- Posting a conspicuous notice for 90 days on the home page of our Practice's Web site that includes a toll-free number for patients to contact for more information; or

- Providing a conspicuous notice in major print or broadcast media in the geographic area where the affected patients likely reside, that includes a toll-free number, active for 90 days, that a patient can call to learn whether or not their PHI may be included in the breach.

e. Urgent Notification – If our Practice determines that a patient should be notified urgently of a breach because of possible imminent misuse of unsecured PHI, our Practice may provide notification to the patient by telephone or other means, as appropriate, in addition to providing the written notice as outlined above.

f. Media Notification – When we reasonably believe that a single breach event affects more than 500 of our patients, notice shall be provided to prominent media outlets serving the area(s) in which our Practice is located, such as through a press release.

g. HHS Notification

i. If a single breach event affects 500 or more patients, notice shall be provided by our Practice without unreasonable delay, but in no case less than 60 days after the breach is discovered, to the Secretary of the U.S. Department of Health & Human Services (HHS). Our Privacy Officer shall use the electronic form available on the HHS Web site, (http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html) when notifying HHS of such breaches.

ii. Our Practice shall maintain an annual log of every breach (determined to require notification under this policy) discovered in a calendar year that affected less than 500 patients. Our Privacy Officer shall notify HHS of such breaches no later than 60 days following the end of each calendar year, using the instructions and electronic form available on the HHS Web site for such notification.

4. Documentation

   a. Our Practice shall maintain documentation related to all breach investigations and notices, including the risk assessment conducted to determine whether a breach notification was required, and shall maintain such documentation for six (6) years after the discovery of the breach.

   b. The documentation maintained for each breach investigation shall include:

      i. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patient affected, if known.

      ii. A description of the types of PHI that were involved in the breach.

      iii. A description of the action taken by our Practice with regard to notification of patients, the media and/or HHS.

      iv. A description of the evidence demonstrating the necessity of any delay in providing notification.

      v. A description of the measures taken by our Practice to mitigate the breach.

      vi. A description of the steps taken by our Practice to prevent future occurrences of that type of breach.

5. Workforce Training – Our Practice shall train all members of our workforce regarding this policy, including how to notify the Privacy Officer of a security incident or possible breach, and shall utilize the Practice's Privacy Policies and Procedures regarding non-retaliation and sanctions related to workforce compliance with this policy.

6. Business Associates – Our Practice's Business Associates shall be required to provide notice to our Privacy Officer of a security incident or possible breach of our Practice's unsecured PHI, without unreasonable delay and within the timeframe established in the Business Associate Agreement. The Business Associate shall be required to provide our Practice with the information necessary for the Practice to conduct a risk assessment and to provide any notice required under this policy, to the extent the Business Associate has such information.

Effective Date: _____

DEFINITIONS

Definition of Breach

A breach is, generally, the acquisition, access, use or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule that compromises the security or privacy of the PHI. Except as provided below, an acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule is presumed to be a breach unless the Covered Entity or Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on the risk assessment as set forth in this policy.

There are three exceptions to the definition of "breach." A breach excludes:

1. The unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate, if such was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.

2. The inadvertent disclosure of PHI by a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the covered entity or business associate and the information is not further used or disclosed in a manner not permitted by the Privacy Rule.

3. A disclosure of PHI where the covered entity or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not reasonably have been able to retain the information.

Unsecured Protected Health Information; Guidance

Covered entities and business associates must only provide the required notification if the breach involved *unsecured protected health information*. Unsecured protected health information is protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified in guidance issued by the Secretary of Health & Human Services. The guidance specifies encryption and destruction as the technologies and methodologies for rendering protected health information unusable, unreadable, or indecipherable to unauthorized individuals. Covered entities and business associates that secure information as specified by the guidance are relieved from providing notifications following the breach of such information. This guidance, found at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html and will be updated annually by HHS.

New Jersey Policy Addendum

Notification under New Jersey's Identity Theft Prevention Act

---

Protection of Social Security Numbers Under the NJITPA

New Jersey's Identity Theft Prevention Act (ITPA) establishes duties regarding Breach of Security and treatment of Social Security numbers and applies to any entity which does business in New Jersey that compiles or maintains Computerized Records that include Personal Information on New Jersey residents. Regulations implementing the ITPA's Breach of Security requirements have not been adopted as of this time. At such time as these regulations are adopted in final form, our Practice will incorporate those requirements in this policy.

NOTE: The IPTA requires notice to the New Jersey Division of State Police in advance of notifying any individuals affected by a Breach of Security. In the event of a Breach of Security triggering the ITPA, our Practice will contact our legal counsel to assist us in expeditiously making the required notification in compliance with current New Jersey law and regulations.

NOTE: Pursuant to proposed regulations, the ITPA requirement to have a comprehensive written security program is not applicable if, as a HIPAA Covered Entity, we are required to have a comprehensive written security program in compliance with the HIPAA Security Rule (see our Practice's HIPAA Security Manual). In addition, the ITPA requirement to disclose to affected persons the misuse of their Personal Information accessed through a Breach of Security is not applicable if, as a HIPAA Covered Entity, we comply with the federal Data Breach Notification Rule as set forth in our Data Breach Notification Policy (to which this New Jersey Policy Addendum is appended).

Pertinent definitions under the ITPA and proposed regulations follow:

"Personal Information" means an individual's first name or first initial and last name linked with any one or more of the following data elements: (1) a Social Security number; (2) a driver's license number or state identification card number; or (3) an account number or credit or debit card number in combination with any required security code, access code, password security question, or authentication device that would permit access to an individual's bank account, investment account or other financial account. Dissociated data that, if linked, would constitute Personal Information is Personal Information if the means to link the dissociated data was accessed in connection with access to the dissociated data. Personal Information does not include publicly available information that is lawfully made available to the general public from Federal, State or local government records or widely distributed media.

"Breach of Security" means unauthorized access to electronic files, including those stored on laptops, MP3 players, personal digital assistants or any other high capacity storage device, media or data containing Personal Information that compromises the security, confidentiality, integrity or availability of Personal Information when access to Personal Information has not been secured by security measures set forth in the comprehensive written information security program of a business or by any other method or technology that renders the Personal Information unreadable or unusable.

"Computerized Records" means records stored in, or transmitted from, a computer as well as those maintained in storage devices related to computers, such as, but not limited to, hard drives, diskettes, memory sticks and flash memory cards.

Communication and Use of Social Security Numbers

Those provisions of the ITPA regulations that have been adopted include restrictions on the communication of Social Security numbers. Our Practice shall comply with those restrictions, as follows:

Our Practice may:

1. Request a Social Security number from an individual, but when asked by the individual, shall state the reason for requesting the individual's Social Security number;
2. Request a Social Security number from an individual, but shall do so in conditions under which the Social Security number will remain confidential;
3. Use a Social Security number for internal verification and administrative purposes, as long as the use does not require the release of the Social Security number to persons not designated by our Practice to perform associated functions allowed or authorized by law;
4. Include a Social Security number 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 number. A Social Security number that is permitted to be mailed under this subsection may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened; and
5. Collect, use or release a Social Security number, as required by or to comply with State or Federal law, or if permitted to do so under applicable law.

Our Practice will not:

1. Publicly post or publicly display an individual's Social Security number or any four or more consecutive numbers taken from the individual's Social Security number;
2. Print an individual's Social Security number on any materials that are mailed to the individual, unless State or Federal law requires the Social Security number to be on the document to be mailed;
3. Print an individual's Social Security number on any card required for the individual to access our services;
4. Require an individual to transmit his or her Social Security number over the Internet, unless the connection is secure or the Social Security number is encrypted; or
5. Require an individual to use his or her Social Security number to access an Internet website, unless a password or unique PIN or other authentication device is also required to access the Internet web site.