Bay Pediatric Clinic P.C.

FINAL RULE HIPAA POLICIES AND PROCEDURES

Effective Date: June 20, 2013 Revision Date Sept 23, 2013 PG 8

INTRODUCTION

On January 25, 2013, the Office of Civil Rights of the U.S. Department of Health and Human Services released a final rule implementing changes to the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules, many of which are required by the HITECH Act (the "Final Rule").

Bay Pediatric Clinic P.C., has adopted these Final Rule HIPAA Policies and Procedures to comply with the Final Rule and with our responsibility to protect individually identifiable health information and the system components that such data resides in under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), the security and privacy regulations implementing HIPAA and HITECH Act, as may be amended from time to time, other federal and state laws protecting confidentiality of health information, professional ethics, and accreditation requirements.

These Final Rule HIPAA Policies and Procedures govern ongoing compliance with HIPAA and supplement, but do not replace Covered Entity's HIPAA Privacy Rule, Security Rule and Breach Notification Rule Policies and Procedures, all of which should be read and implemented together. In the event of any conflict or inconsistency between these Final Rule HIPAA Policies and Procedures and Covered Entity's current HIPAA Policies and Procedures, these Final Rule HIPAA Policies and Procedures shall control. Covered Entity's HIPAA Policies and Procedures which are not amended hereby shall remain in full force and effect, and as amended the Covered Entity reaffirms them and confirms its obligations thereunder. These Final Rule HIPAA Policies and Procedures are not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of the HIPAA Privacy, Security or Breach Notification Rule (subparts C, D and E of 45 CFR part 164).

The law requires us to keep our patients' protected health information ("PHI") private in accordance with our Notice of Privacy Practices ("Notice") for as long as the Notice remains in effect. Covered Entity takes its patients' privacy seriously and expects its employees, independent contractors, agents and business associates to do the same. If you have any questions regarding privacy of PHI or these Final Rule HIPAA Policies and Procedures, please contact the Privacy Official.

POLICIES AND PROCEDURES

Notice of Privacy Practices.

Bay Pediatric Clinic P.C., shall timely make modifications to and redistribute its Notice of Privacy Practices, as required by the Final Rule.

Training

Covered Entity must train all members of its workforce on the Policies and Procedures implemented in connection with the Final Rule, as necessary and appropriate for the members of the workforce to carry out their functions within Covered Entity, within ten (10) business days of the Effective Date of these Final Rule HIPAA Policies and Procedures. Each member of the workforce will be trained on all HIPAA Policies and Procedures within a reasonable period of time after the person joins Covered Entity's workforce and periodically on designated dates at least once every twelve (12) month thereafter; and each member of Covered Entity's workforce whose functions are affected by a material change in Covered Entity's HIPAA Policies or Procedures will be trained within a reasonable period of time after the material change becomes effective. Further, Covered Entity shall periodically provide HIPAA

training to all of its workforce members. Covered Entity must document that the training has been provided.

Required by Law.
Bay Pediatric Clinic P.C., may use or disclose medical information when Bay Pediatric Clinic P.C., is required to do so by law, without individual's authorization or opportunity to agree or object. For example, PHI may be released when required by privacy laws, workers' compensation or similar laws, public health laws, court or administrative orders, subpoenas, certain discovery requests, or other laws, regulations or legal processes. Under certain circumstances, Bay Pediatric Clinic P.C., may make limited disclosures of PHI directly to law enforcement officials or correctional institutions regarding an inmate, lawful detainee, suspect, fugitive, material witness, missing person, or a victim or suspected victim of abuse, neglect, domestic violence or other crimes. Bay Pediatric Clinic P.C. may disclose PHI to the extent reasonably necessary to avert a serious threat to a patient's health or safety or the health or safety of others. Bay Pediatric Clinic P.C., may disclose PHI when necessary to assist law enforcement officials to capture a third party who has admitted to committing a crime against the patient or who has escaped from lawful custody. Bay Pediatric Clinic P.C., may also disclose PHI to a school about an individual who is a student or a prospective student of the school if the PHI is limited to proof of immunization, the school is required by law to have such proof of immunization prior to admitting the individual, and the Bay Pediatric Clinic P.C., obtains and documents an agreement to the disclosure from either the individual or, if the individual is a minor, from the individual's parent, guardian or other person acting on individual's behalf if the individual is a minor. Contact the Privacy Official prior to making any use or disclosure under this section.

Deceased Individuals.
Bay Pediatric Clinic P.C., must comply with the requirements of the HIPAA Privacy Rule with respect to PHI of a deceased individual for a period of 50 years following the death of the individual. This time limitation does not override or interfere with applicable State or other laws that provide greater protection for such information. Except where prohibited by applicable State or other applicable law, Covered Entity may destroy the PHI of a deceased individual after a period of 50 years following the death of the individual. Deceased individual's record should be noted with the date of death.

Authorizations.
Bay Pediatric Clinic P.C., may use or disclose PHI for any purpose consistent with a written authorization they receive from patient. With limited exceptions, a prior written authorization is required for use and disclosure of psychotherapy notes, marketing and sale of PHI. We may not condition treatment on the receipt of any authorization from a patient. A patient may revoke an authorization at any time by writing to the Privacy Official. The revocation will be effective only prospectively, and will not affect any uses or disclosures made prior to revocation and pursuant to the authorization. Prior to releasing information pursuant to an authorization, We must confirm that the authorization is complete and valid and that no revocations have been placed in the file. Our minimum disclosure policy does not apply to uses or disclosures made pursuant to an authorization. The PHI used or disclosed will be consistent with the information authorized to be used or disclosed.

Contact the Privacy Official prior to making any use or disclosure under this section. Also, See Prohibition on Sale of Electronic Health Records or PHI, Marketing and Fundraising Policies for additional matters related to patient authorizations.

Continuing Care.
Bay Pediatric Clinic P.C., may provide patients with appointment reminders and information concerning health issues, benefits and services, or treatment alternatives based upon their PHI. Bay Pediatric Clinic P.C., may disclose PHI to a business associate to assist us in these activities. Where the sending of such communications involves receipt of financial remuneration by us, Bay Pediatric Clinic P.C. will

notify the individual of such communications through the authorization process described under the Marketing policy.

Access and Copies.
A patient or patient's personal representative has a right to review and/or obtain copies of PHI in designated record sets, and the right to direct Bay Pediatric Clinic P.C., to transmit a copy of PHI directly to another designated person, by requesting access or copies in writing to Privacy Official. The request should signed by the patient or patient's representative, and contain the patient's name, address, and daytime telephone number; if submitted by patient's personal representative, proof of status; time period of the request, and form of access or copies requested (on-site, electronic, mailed copy, etc.); and the name of the person to whom the PHI should be sent, if applicable.

If the requested PHI is maintained in one or more designated record sets electronically and if the request is for an electronic copy of such information, Bay Pediatric Clinic P.C., must provide copies or access to the PHI in the electronic form and format requested, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by Covered Entity and the requestor. In these cases, to the extent possible, the requestor will be provided with electronic information in the format readable by a computer, such as MS Word or Excel, text, HTML, or PDF, among other formats. If an individual requests a form of electronic copy that we are unable to produce, then we will offer other electronic formats that are available on its systems. If the individual declines to accept any of the electronic formats that are readily producible by us, then we will provide a hard copy as an option to fulfill the access request.

Requests must be granted or denied within thirty (30) days from the date a request is received, or within an additional thirty (30) days if we need more time to respond, provided that a timely notice of longer processing is sent during the first thirty (30) day period with reasons for the delay and the date by which the Bay Pediatric Clinic P.C., will complete its action on the request. If the request is denied, we will provide a patient or representative a written basis for the denial, including the PHI to which the denial applies, if applicable, the right to review the denial, and how the patient may complain to Bay Pediatric Clinic P.C., or the Secretary of HHS. The patient or patient's personal representative may only request a review of a denial that was based on safety concerns (i.e., endangering the life or physical safety of the patient or another person). The appeal will be reviewed within thirty (30) days to determine whether the denial was appropriate.

Requests for Restrictions.
A patient or patient's personal representative may request that Bay Pediatric Clinic P.C., place restrictions on the use or disclosure of PHI to carry out treatment, payment or healthcare operations, permitted disclosures to family members, representatives or other third parties, and disclosures for disaster relief purposes. You also have the right to request a limit on disclosures of your PHI to others, such as patient registries and HIEs. All requests must be in writing, and should contain the name, address, and daytime phone number, and either the manner in which the requestor wishes Bay Pediatric Clinic P.C., to restrict its uses and disclosures of PHI for treatment, payment or health care operations, or the persons involved in their care to whom we should not disclose PHI. Bay Pediatric Clinic P.C., is not required to honor such a request, except that we must agree to a request to restrict disclosure of PHI to a health plan if the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law and the PHI pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the Bay Pediatric Clinic P.C., in full.

The Privacy Official will determine if the restriction is feasible, and will notify the requestor accordingly. Bay Pediatric Clinic P.C., will be bound by restrictions only if it agrees to do so in writing signed by Privacy Official. Even if the Bay Pediatric Clinic P.C., agreed to a restriction, except where

it was required to do so, if the individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide the emergency treatment, Bay Pediatric Clinic P.C., may use the restricted PHI, or may disclose such information to a health care provider, to provide such treatment to the individual if the covered entity requests that such health care provider not further use or disclose the information.

If Bay Pediatric Clinic P.C., determines it no longer wishes to continue operating in accordance with an agreed-to restriction, except for the restriction that we must agree to as provided above, it may terminate the restriction by obtaining oral or written assent from the requestor, or notify the requestor that the agreed-to restriction is terminated. The Privacy Official must document all restrictions, termination of restrictions, and timely notify any business associates of the restrictions or termination thereof.

Calculation of Fees for Providing Copies of PHI to Patients and Patients' Personal and Authorized Representatives.
HIPAA and Michigan Medical Records Access Act ("MMRAA") permit us to impose fees for providing copies of PHI to patients and their personal and authorized representatives. Contact Privacy Official with questions about copying fees.

Requests by Patients: If an individual requests a copy of his or her PHI, agrees to receive a summary or explanation of such information, or directs Covered Entity to transmit such a copy (or a summary or explanation of such information) directly to another entity or person, we are allowed to charge a reasonable, cost-based fee, based only on the cost of: (i) Labor for copying the PHI requested by the individual, whether in paper or electronic form; (ii) Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media, (iii) Postage, when the individual has requested that the PHI or summary or explanation be mailed; and (iv) Preparing the explanation or summary of the PHI if the individual agrees in advance to receive such an explanation or summary and agrees in advance to the fees to be charged for such summary or explanation. The reasonable, cost-based fee may *not*: (i) Include costs associated with searching for and retrieving the requested information or an "initial fee" that is unrelated to the permissible costs described above; or (ii) Exceed the maximum fees prescribed by the MMRAA, a schedule of which is published by the Michigan Department of Community Health. The latest version of the MMRAA fee schedule is attached.

Requests by Personal and Authorizes Representatives: A person who has the authority to make health care decisions for the individual who is the subject of the PHI must be treated as if he or she were the patient for purposes of HIPAA. Therefore, if a request for copies is made by a person with such authority, we will charge the same fee described in "Requests by Patients" section, above. If a request for copies of PHI is made by (i) An attorney or other person who is not authorized to make health care decisions for the patient but possesses written authorization from the patient to obtain a copy of patient's PHI or parts thereof such as patient's medical record, or (ii) If the patient is deceased, his or her personal representative, heirs at law or the beneficiaries of the patient's life insurance policy, we can charge fees, including an "initial fee", prescribed by the MMRAA.

Business Associates.
Bay Pediatric Clinic P.C., must have a signed written agreement with each person or entity who in providing services to the Bay Pediatric Clinic P.C., is considered a business associate under the HIPAA Privacy Rule, including those who create, receive, maintain, or transmit PHI for or on behalf of the Bay Pediatric Clinic P.C., and who is not a member of the Bay Pediatric Clinic P.C., workforce, Only business associates that have signed a business associate agreement may create, receive, maintain,

or transmit PHI for or on behalf of the Bay Pediatric Clinic P.C., to the extent necessary to perform services for Bay Pediatric Clinic P.C..

If Bay Pediatric Clinic P.C., and a business associate entered into a HIPAA-compliant business associate agreement prior to January 25, 2013, then on or before September 22, 2014 Covered Entity will amend it or enter into a new business associate agreement that complies with the provisions of the Final Rule. Bay Pediatric Clinic P.C., will include the provisions required by the Final Rule in any business associate agreement that is modified or actively renewed between March 26, 2013 and September 23, 2013. In all other cases, Bay Pediatric Clinic P.C., will enter into business associate agreements that comply with the Final Rule no later than September 23, 2013.

If Bay Pediatric Clinic P.C., learns of a business associate's potential breach or violation of its business associate agreement (either through a patient complaint, during a performance audit, or otherwise), it will investigate the potential or alleged breach and violation, and upon determining that there was a material breach or violation of the business associate's obligations, will work with the business associate to end the violation or to cure the breach, as applicable, and if such steps were unsuccessful, terminate the business associate agreement and/or other arrangement, of feasible.

Prohibition on Sale of Electronic Health Records or PHI.
Except as provided below, Bay Pediatric Clinic P.C., may not sell PHI and directly or indirectly receive remuneration (which includes the receipt of nonfinancial as well as financial benefits) from or on behalf of the recipient of the PHI in exchange for the PHI of an individual unless Covered Entity obtains from the individual, in accordance with section 45 CFR 164.508, a valid authorization that includes a statement that the disclosure will result in direct or indirect remuneration to the Covered Entity, and, if applicable, the specific remuneration Covered Entity will receive.

A sale of PHI does not include, and the foregoing restriction does not apply to, the following disclosures of PHI:

i. Disclosure for public health purposes (as described in 45 CFR 164.512(b) or 164.514(e)).

ii. Disclosure for research pursuant to 45 CFR 164.512(i) or 164.514(e), where the only remuneration received by the Covered Entity is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purposes.

iii. Disclosure for treatment of the individual and payment purposes.

iv. Disclosure for the sale, transfer, merger, or consolidation of all or part of Covered Entity with another covered entity, or an entity that following such activity will become a "covered entity" for HIPAA purposes, and due diligence related to such activity, provided such disclosure is otherwise made pursuant to the HIPAA Privacy Rule.

v. Disclosure to or by a business associate for activities involving the exchange of PHI that the business associate undertakes on behalf of and at the specific request of Covered Entity pursuant to a business associate agreement, and the only remuneration provided is for the performance of such activities.

vi. Disclosure in response to a request by an individual for a copy of the individual's PHI pursuant to 45 CFR 164.524 or for an accounting of disclosures pursuant to 45 CFR 164.528.

vii. Disclosure required by law, as permitted under 45 CFR 164.512(a).

viii. Disclosure for any other purpose permitted by and in accordance with the HIPAA Privacy Rule, where the only remuneration received by the Covered Entity or business associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee otherwise expressly permitted by other law.

Covered Entity shall describe in its Notice of Privacy Practices that any disclosure of PHI that is a sale of PHI requires an authorization from an individual.

Marketing.
Bay Pediatric Clinic P.C., must obtain an authorization for any use or disclosure of PHI for all marketing or subsidized communications that market a health related product or service, except if the communication is in the form of:

i. A face-to-face communication made by a covered entity to an individual; or

ii. A promotional gift of nominal value provided by the covered entity.

If marketing involves any financial remuneration to the Bay Pediatric Clinic P.C., from a third party, the authorization must state that such remuneration is involved. For purposes of this Policy, financial remuneration means direct or indirect payment from or on behalf of a third party whose product or service is being described, and direct or indirect payment does not include any payment for treatment of an individual. Bay Pediatric Clinic P.C., shall describe in its Notice of Privacy Practices the types of marketing communications that require an authorization from an individual.

Marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service, except where the communication is made:

i. To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the recipient of the communication, only if any financial remuneration received by Bay Pediatric Clinic P.C., in exchange for making the communication is reasonably related to the Covered Entity's cost of making the communication.

ii. For the following treatment and health care operations purposes, except where the Covered Entity receives financial remuneration in exchange for making the communication:

a. For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;

b. To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the Covered Entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

c. For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

Fundraising.
If Bay Pediatric Clinic P.C., indicates in its Notice of Privacy Practices that it intends to contact the individual to raise funds for Bay Pediatric Clinic P.C., and that the individual has a right to opt out of receiving such communications, Covered Entity may contact the individual, or use or disclose to a business associate or to an institutionally related foundation, the following PHI for the purpose of raising funds for its own benefit (such as, for example, appeals for money, sponsorship of events, etc.), without first obtaining an authorization from an individual:

i. Demographic information relating to an individual, including name, address, other contact information, age, gender, and date of birth;

ii. Dates of health care provided to an individual;

iii. Department of service information;

iv. Treating physician;

v. Outcome information; and

vi. Health insurance status.

Bay Pediatric Clinic P.C., may not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications.

With each fundraising communication made to an individual by or on behalf of Bay Pediatric Clinic P.C., individual must be provided with a clear and conspicuous opportunity to elect not to receive any further fundraising communications, which the individual can implement without undue burden or result in more than a nominal cost to the individual. The opt out method may include the use of a toll-free phone number, an email address, mailing a pre-printed pre-paid post card, or similar opt out mechanisms that provide the individual with simple, quick, and inexpensive ways to opt out of receiving further fundraising communications, but may not include a requirement that the individual write and send a letter to us asking not to receive further fundraising communications. Bay Pediatric Clinic P.C., may employ multiple opt out methods, allowing individuals to determine which opt out method is the simplest and most convenient for them, or a single method that is reasonably accessible to all individuals

wishing to opt out. Bay Pediatric Clinic P.C., shall honor the individual's request not to receive further fundraising communications.

Bay Pediatric Clinic P.C. may provide an individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications. Where an individual who has opted out of fundraising communications makes a donation to Bay Pediatric Clinic P.C., it does not serve, absent a separate election to opt back in, to automatically add the individual back onto the mailing list for fundraising communications.

The Privacy Official is responsible to establish and implement the opt out methods, considering the size of the population to which Covered Entity will be sending the communications, the geographic distribution, and any other factors that may help determine which opt out method(s) is most appropriate and least burdensome to individuals, the opt in methods, and the enforcement of the individual's decision to opt out or opt in.

HITECH Act.
The HITECH Act introduced many proposed changes to the HIPAA Privacy, Security and Breach Notification Rules, some of which have become effective and some may become effective in the near future. Covered Entity is committed to complying with the HITECH Act and its implementing regulations, as may be applicable to its medical practice, will monitor HITECH Act developments and implementation requirements, and will update its HIPAA policies and procedures to ensure compliance with the applicable provisions of the HITECH Act and its implementing regulations.

ENFORCEMENT

All workforce members, including officers and employees, of Covered Entity **must** adhere to these Policies and Procedures, except for the HITECH Act Policy, which is the responsibility of the Privacy Official. Violations of any of these Policies and Procedures are grounds for disciplinary action up to and including termination of employment and other sanctions in accordance with Covered Entity's HIPAA Sanction Policy and personnel rules and regulations.

Breach Notification/ 9/23/2013

Bay Pediatric Clinic has an obligation to notify patients if there is a breach of their PHI is expanded and clarified under the new rules. Breaches are reviewed and presumed reportable unless after completing a risk analysis applying four factors, it is determined, that there is a "low probability of PHI compromise."

Four factors

- The nature and extent of the PHI involved-issues to be considered include the sensitivity of the information from a financial or clinical perspective
- The person who obtained the unauthorized access and whether that person has an independent obligation to protect the confidentiality of the information
- Whether the PHI was actually acquired or accessed, determined after conducting a forensic analysis
- The extent to which the risk has been mitigated, such as by obtaining a signed confidentiality agreement from the recipient.

Treatment, Payment and Health Care Operations.

Covered Entity has the right to use and disclose your PHI for all activities that are included within the definitions of “treatment”, “payment” and “health care operations” as defined in the HIPPA Privacy Rule.

Treatment. Covered Entity may use or disclose your PHI to any physician or other health care provider involved with the medical services provided to you. This includes disclosures of your PHI to other healthcare providers through electronic exchanges such as patient registries and Health Information Exchanges (HIEs).