HIPAA Security, Privacy and Breach Notification Policies &

Procedures for Protected Health Information

Bellevue Bone & Joint Physicians, PLLC

PURPOSE

The American Recovery and Reinvestment Act of 2009 ("ARRA"), signed into law on February 17, 2009, significantly expanded the privacy and security requirements under the Health Information Portability and Accountability Act ("HIPAA"). These regulations, as well as the Health Information Technology for Economic and Clinical Health ("HITECH") breach notification requirements are now directly applicable to Business Associates, like Bellevue Bone & Joint Physicians. The governing statutes encourage Covered Entities that contract with Business Associates to request a copy of the Business Associate's HIPAA Privacy and Security Policy; therefore these policies may be distributed externally by the Privacy Committee to Bellevue Bone & Joint Physicians clients, as needed.

The following Policies and Procedures will govern the use and disclosure of Protected Health Information ("PHI") at Bellevue Bone & Joint Physicians, as well as what steps will be taken in the event unsecured PHI is breached in a manner prohibited under HIPAA. No third-party rights (including but not limited to rights of covered entities, plan administrators, participants, beneficiaries, covered dependents, brokers or other business associates) are intended to be or are created by these guidelines. Bellevue Bone & Joint Physicians reserves the right to amend or change these Policies and Procedures at any time (including retroactively). These Policies and Procedures are solely for purposes of ensuring that Bellevue Bone & Joint Physicians employees know what is required by ARRA, HITECH and HIPAA with respect to the treatment of PHI and are not intended to address obligations or requirements under any other law. To the extent these Policies and Procedures set forth requirements above and beyond what is required by ARRA, HITECH, HIPAA or other federal or state laws, they are not binding upon Bellevue Bone & Joint Physicians or its employees.

TRAINING

Every employee will receive appropriate HIPAA privacy and security compliance training and will sign a written acknowledgement that he/she has received and reviewed these Policies and Procedures and that he/she understands and agrees to abide by the guidelines contained herein. Additionally, certain employees in supervisory positions will receive further HIPAA training regarding discovery and prevention of security and privacy violations.

DEFINITIONS

Protected Health Information ("PHI") – means information, in any format, that is created or received by Bellevue Bone & Joint Physicians and relates to the past, present, or future physical or mental health or condition of a participant; the provision of health care to a participant; or the past, present, or future payment for the provision of health care to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant.

Electronic PHI ("ePHI") - a subset of PHI that is created, received, maintained or transmitted in electronic format. All ePHI is Protected Health Information and is subject to the HIPAA privacy, security and breach notification requirements.

Secured PHI - PHI that has been rendered unusable, unreadable, or indecipherable to

unauthorized individuals by either encryption or destruction by a method approved by the National Institute of Standards and Technology.
Unsecured PHI - any PHI that is not secured using one of the HHS-approved technologies or methods (encryption or destruction).
Use - the sharing, employment, application, utilization, examination, or analysis of PHI, in oral, written, electronic or other format.
Disclosure - any release, transfer, provision of access to, or divulging in any other manner of PHI to persons outside of Bellevue Bone & Joint Physicians.
Breach – the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI in that the disclosure of the information poses a significant risk of financial, reputational, or other harm to the individual.

HIPAA SECURITY POLICIES AND PROCEDURES

It is the policy of Bellevue Bone & Joint Physicians to fully comply with the HIPAA Security Rule, including to: (1) ensure the confidentiality, integrity, and availability of all electronic PHI ("ePHI") that Bellevue Bone & Joint Physicians creates, receives, maintains, or transmits; (2) protect against reasonably anticipated threats or hazards to the security or integrity of ePHI; (3) protect against reasonably anticipated uses or disclosures of ePHI that are not permitted or required under the HIPAA Privacy Rule; and (4) ensure compliance with the HIPAA Security Rule by all Bellevue Bone & Joint Physicians employees.
It is the policy of Bellevue Bone & Joint Physicians to exercise the discretion afforded to it by HHS to select security measures that Bellevue Bone & Joint Physicians believes are best suited to reasonably and appropriately meetthe standards and specifications set forth by the HIPAA Security Rule. Those security measures include appropriate safeguards such as limiting building access, implementing firewalls and utilizing password protections, as these access controls are recognized by HHS as important for safeguarding PHI. It is the policy of Bellevue Bone & Joint Physicians to regularly review its IT practices and infrastructure and to consider appropriate methods to enhance security measures.

HIPAA PRIVACY POLICIES AND PROCEDURES

I. USE AND DISCLOSURE OF UNSECURED PHI

A. Access to PHI - All Bellevue Bone & Joint Physicians employees are authorized to access PHI to the extent performance of their job functions reasonably requires such access and where access is necessary in furtherance of legitimate, HIPAA-approved purposes of payment, treatment and health care operations. Employees may not access PHI except in accordance with these Policies and Procedures and only in furtherance of proper business-related activities.

B. Employees Shall Abide by the HIPAA "Minimum Necessary" Standard - It is the policy of Bellevue Bone & Joint Physicians that all employees abide by the HIPAA Minimum Necessary Standard, i.e. that the amount and type of PHI requested, accessed,

used and/or disclosed shall be limited to the "minimum necessary" information that is needed to accomplish the intended, authorized purpose of the use, disclosure or request. Use and disclosure to other authorized Bellevue Bone & Joint Physicians employees, plan administrators, authorized representatives of the Covered Entity, brokers and/or other business associates will be made in accordance with the Minimum Necessary Standard.

C. Uses and Disclosures Excepted from the Minimum Necessary Standard – The following procedures should be followed in situations where the Minimum Necessary Standard does not apply:

1. Use and Disclosure to Parent or Legal Guardian of Minor Child Participant – Employees may disclose PHI to the parent or legal guardian of a minor child participant, so long as appropriate steps are taken to verify the identity of the person making the request and to confirm relationship between that person and the minor child.

2. Use and Disclosure to Third-Parties Pursuant to Written Authorization of the Participant - Employees shall not disclose PHI in response to a request from a third-party claiming to have authorization from the participant unless sufficient written authorization has been verified and the disclosure has been approved by the Privacy Committee Chairperson.

a. Personal Representatives - If a PHI disclosure request is made by a participant's personal representative, employees shall refer the initial request to the Privacy Committee Chairperson to verify that proper documentation and authorization has been obtained before making the disclosure.

b. Use and Disclosure to Spouses, Family Members or Friends - Employees shall not disclose PHI to spouses, family members or friends of participants, absent express written authorization from the participant. All requests for the disclosure of PHI received from a spouse, family member or friend (excluding requests from the parent or legal guardian of a minor child participant) shall be referred to the Privacy Committee Chairperson in order to ensure that the proper authorization has been obtained before making the disclosure.

3. Disclosures to HHS, Law Enforcement or Other Administrative or Judicial Authorities - Employees shall not disclose PHI in response to requests by HHS, law enforcement agents or other government or administrative authorities. Any and all such requests (including subpoenas, court orders, discovery requests, public health, criminal or civil investigations, etc.) shall be referred to the Privacy Committee Chairperson.

D. Access and Amendment to a Participant's Own PHI – HIPAA requires that participants be afforded the opportunity access certain PHI within a Designated Record Set and to amend or correct their own PHI, upon request. The Designated Record Set includes enrollment, payment, and claims adjudication records, and

other PHI used by or for the Plan to make coverage decisions about an individual. If a participant submits a request to access and/or amend their own PHI, the Privacy Committee Chairperson will respond to such requests in the manner set forth by HIPAA.

E. Verification of the Identity of the Individual Requesting PHI – Employees shall take reasonable steps to verify the identity and authority of all persons requesting access to PHI before making any disclosure. If the identity or authority of the person making the request is at all in question, employees are directed to contact the Privacy Committee Chairperson.

II. POLICIES AND PROCEDURES IN THE EVENT OF A POTENTIAL BREACH OF UNSECURED PHI

It is the policy of Bellevue Bone & Joint Physicians that all employees will access, use and disclose PHI only as permitted under HIPAA, and that all employees shall be vigilant with respect to guarding PHI. However, in the event that a potential breach of unsecured PHI occurs, the following policies and procedures shall be followed.

A. Step 1 – DISCOVERY

i. A breach of PHI will be deemed "discovered" as of the first day Bellevue Bone & Joint Physicians knows of the breach or, by exercising reasonable diligence, would or should have known about the breach.

ii. If a potential breach is discovered, it is very time sensitive and must be immediately reported.

B. Step 2 – INTERNAL REPORTING

i. If you believe that a potential breach of PHI has occurred, you must immediately notify the Privacy Committee Chairperson.

ii. Please provide all of the information you have available to you regarding the potential breach, including names, dates, the nature of the PHI potentially breached, the manner of the disclosure (fax, email, mail, verbal), all employees involved, the recipient, all other persons with knowledge, and any associated written or electronic documentation that may exist.

iii. Notification and associated documentation may itself contain PHI and should only be given to the Chairperson, or another member of the Privacy Committee.

iv. Please do not discuss the potential breach with anyone else, and do not attempt to conduct an investigation. These tasks will be performed by the Privacy Committee.

C. Step 3 – INVESTIGATION

i. Upon receipt of notification of a potential breach the Chairperson, or his/her designee, shall promptly conduct an investigation.

ii. The investigation shall include interviewing employees involved, collecting written documentation, and completing all appropriate

documentation.

iii. The Chairperson shall retain all documentation related to potential breach investigations for a minimum of six years

D. Step 4 - RISK ASSESSMENT AND RECOMMENDATION TO THE COMMITTEE

After the investigation is complete, the Privacy Committee Chairperson will perform a Risk Assessment. The purpose of the Risk Assessment is to determine if a use or disclosure of PHI constitutes a breach and requires further notification to the Covered Entity. The Chairperson shall appropriately document the Risk Assessment and make a recommendation to the full Committee regarding whether notification to the Covered Entity of the potential breach would be prudent.

A "reasoned judgment" standard will be applied to the Risk Assessment, which shall be fact specific, and shall include consideration of the following factors:

- Did the disclosure involve Unsecured PHI in the first place?
- Who impermissibly used or disclosed the Unsecured PHI?
- To whom was the information impermissibly disclosed?
- Was it returned before it could have been accessed for an improper purpose?
- What type of Unsecured PHI is involved and in what quantity?
- Was the disclosure made for any improper purpose?
- Is there the potential for significant risk of financial, reputational, or other
- harm to the individual whose PHI was disclosed?
- Was immediate action taken to mitigate any potential harm?
- Do any of the specific breach exceptions apply?

E. Step 5 – FINAL DETERMINATION BY THE PRIVACY COMMITTEE

The Bellevue Bone & Joint Physicians Privacy Committee shall have final authority to determine whether a breach of unsecured PHI occurred and what, if any, further action is warranted.

F. Step 6 – NOTIFICATION TO COVERED ENTITY - In the event that the Privacy Committee determines that notice to the Covered Entity is warranted, the Chairperson shall promptly prepare and transmit a CE Notice.

i. Content - The CE Notice shall include:

1. Identification of each individual whose Unsecured PHI is believed to have been breached, the date of the disclosure, the facts and circumstances surrounding the disclosure, and all associated documentation.

2. The CE Notice shall include all other available information known to Bellevue Bone & Joint Physicians that the Covered Entity will be required to include in its own Notice to the individual(s).

3. If additional information regarding the breach is later discovered by Bellevue Bone & Joint Physicians, that information will be promptly provided to the Covered Entity.

4. The CE Notice shall be sent first class mail, return receipt requested, and the receipt and a copy of the CE Notice shall be kept with related documentation.

5. Upon receipt of the CE Notice from Bellevue Bone & Joint Physicians, it is the obligation of the Covered Entity to notify affected individuals, HHS, and/or the media unless otherwise specifically agreed upon by contract.

ii. Timing of Notification - Bellevue Bone & Joint Physicians shall notify the Covered Entity "without unreasonable delay" but no later than 60 days after discovery of the breach. The Bellevue Bone & Joint Physicians Services Agreement provides that Bellevue Bone & Joint Physicians is an independent contractor; therefore the Covered Entity's time to provide the requisite notice begins to run on the date that Bellevue Bone & Joint Physicians notifies the CE of the breach.

1. Unjustified Delay - If it appears to the Chairperson that the investigation will not be completed within a reasonable time, the Covered Entity will be notified before completion of the investigation.

2. Law Enforcement Delay - A delay in notification is permissible if a law enforcement official states that a breach notification would impede a criminal investigation or cause damage to national security.

a. In that event, the law enforcement statement must be in writing and must specify the length of the delay required.

b. If the request for a delay in notification is oral, Bellevue Bone & Joint Physicians must document the statement and request written confirmation within 30 days. If no written request for a delay is received within that time, Bellevue Bone & Joint Physicians must send notification of the breach to the Covered Entity.

G. Step 7 – DOCUMENTATION - All phases of the process must be documented in detail on a case-specific basis, in a manner sufficient to demonstrate that all appropriate steps were completed. All supporting documentation associated with the potential breach shall be kept on file for a period of 6 years.

H. SANCTIONS

Bellevue Bone & Joint Physicians employees who fail to fully comply with Bellevue Bone & Joint Physicians HIPAA Privacy, Security and Breach Notification Policies and Procedures contained herein will be subject to sanctions as deemed appropriate by management.