Valley Bone & Joint Clinic

HIPAA Privacy Policy *(Revised Feb. 4, 2015)*

1. PURPOSE

Valley Bone & Joint Clinic is committed to protecting the rights of our patients. In compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH") and applicable federal and state laws and regulations, this policy sets forth VBJC's practice of implementing, enforcing, updating, and documenting its compliance with HIPAA policies and procedures.

- VBJC will implement policies and procedures that are reasonably designed to ensure compliance with the HIPAA standards, requirements and implementation specifications.

-VBJC will monitor changes to HIPAA and will promptly revise its policies and procedures and, if required, its Notice of Privacy Practices.

-VBJC will maintain documentation required for HIPAA compliance for a minimum period of six (6) years from the date of the creation of the document.

-VBJC employees who violate these policies will be subject to disciplinary action up to and including termination. Anyone who knows or has reason to believe that another person has violated any of these policies should report the matter promptly to his or her supervisor or the Privacy Manager.

2. SCOPE

a. This policy applies to all VBJC employees, contractors, student, and volunteers.

b. This policy describes VBJC's objectives and policies regarding maintaining the privacy of patient health information.

3. REFERENCES

a. VBJC Technology Policy

b. Patient Notice of Privacy Policy

c. Business Associate Agreement Form and various Patient Privacy Request Forms

4. DEFINITIONS

Authorization: a patient's written permission to allow the Medical Center to use or disclose specified protected health information. Different types of activities (e.g. fundraising, research) have specific authorization requirements.

Breach: the acquisition, access, use, or disclosure of protected health information in a manner not permitted by the Privacy Rule.

Business Associate: a company or individual who performs a function or service on behalf of VBJC that creates, receives, maintains, or transmits protected health information in connection with that function or service.

Business Associate Agreement: a contract between VBJC and a Business Associate that meets the requirement specified in the Privacy Rule.

Disclosure: the release, transfer, provision of access to, or divulging of information, in any manner, outside the entity holding the information.

Employee: anyone, including physicians, who are employed by Valley bone & Joint Clinic (VBJC).

Health Information: means any information, including genetic information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Health Plan: a health plan, or insurer, means an individual or group plan that provides, or pays the cost of, medical care. This can include: a group health plan, an HMO, Medicare Part A or B, Medicaid, or a private health insurer.

Incident or Privacy/Security Incident: the unauthorized access, use, disclosure, theft, loss, modification, or destruction of protected health information or personally identifiable information. Incidents do not always arise to the level of a breach.

Limited Data Set: a set of data in which most of the personal identifiers have been removed. Certain identifiers must be removed for a data set to be considered a limited data set, which is used only internally.

Payment: the activities undertaken by VBJC to obtain or provide reimbursement for health care services it has provided. This includes billing, collection activities, and billing review activities.

Personal Representative: a person who may legally act with authority on behalf of another person in making decisions about health care.

Personally identifiable information: a person's first name or first initial and last name in combination with any of the following: Social Security Number; Driver's license number or other identification number; Account number or credit/debit card number; address; birthdate; email address; or full face photograph.

Privacy Manager: refers to the VBJC designated HIPAA Privacy Official, who is responsible for overseeing compliance with HIPAA policies and procedures.

PHI or Protected health information: any information (including demographic information) created, maintained, received, or transmitted by the VBJC that relates to health status, provision of health care or payment for health care and can be used to identify the individual.

Treatment: the provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.

5. RESPONSIBILITIES

a. **VBJC President and Physicians**

- Establish program objectives
- Approve privacy policy
- Provide training for work force
- Enforce sanctions
- Designate Privacy Manager

b. **Privacy Manager**

- Develops privacy policies and procedures
- Coordinates and implements policy through organization's departments
- Oversees training
- Receives and processes privacy complaints
- Processes individual rights requests (access/copy protected health information (PHI), amend PHI, restrict use/disclosure of PHI, confidential communication request, accounting of disclosures, and filing of complaints)
- Ensures retention of HIPAA policies and procedures, complaints, and investigative materials to meet compliance requirements.

c. **Employee Responsibilities**

- Understand and comply with VBJC's policies regarding patient confidentiality and privacy.

6. DESIGNATED RECORD SET

a. Electronic Medical Record - stored off site with IMS software.

b. Billing records - stored off site with IMS software.

c. Electronic copies of old Bradoc EMR and old paper charts in storage.

7. NOTICE OF PRIVACY PRACTICES (NPP)

a. VBJC will develop and distribute to its patients a Notice of Privacy Practices (NPP) describing the uses and disclosures of Protected Health Information (PHI) that may be made by the clinic, the patient's rights, and VBJC's duties with respect to PHI.

b. VBJC will make available the NPP to any person upon request, and post the NPP in a clear and prominent location, and make the NPP electronically available on its' website.

d. The organization will make a "best effort" attempt to receive acknowledgment of receipt of NPP from each patient and document such in the patient's medical record.

8. MINIMUM NECESSARY POLICY

a. Whenever VBJC discloses Protected Health Information ("PHI"), reasonable efforts will be made to limit the amount of PHI disclosed to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. A patient's entire medical record will only be provided if the entire medical record can be specifically justified as the minimum amount necessary under the particular circumstance. Information that exceeds minimum necessary will be redacted prior to release.

b. For disclosures made on a routine and recurring basis, VBJC will limit employee access to PHI to the minimum necessary through the appropriate safeguards, including but not limited to restricting user access to systems that contain PHI based on job function and duties, and providing only the minimum necessary access level consistent with those duties.

9. **USE AND/OR DISCLOSURE OF PROTECTED HEALTH INFORMATION**

a. VBJC may use and disclose Protected Health Information ("PHI"): for Treatment, Payment and Health Care Operations; to the patient or pursuant to the patient's valid Authorization; to a legal Personal Representative of the patient; to family and friends involved in the patient's care and for notification purposes as permitted by law; to Business Associates subject to a Business Associate Agreement; to create information that is not individually identifiable health information (known as De-Identified Information) or Limited Data Sets; as otherwise permitted or required by state or federal laws or regulations.

b. VBJC will use reasonable professional judgment to verify the identity and authority of unknown person requesting access to Protected Health Information ("PHI"). Employees must obtain any required documentation, statements, and representations (oral or written) from the requestor prior to permitting

c. access or disclosure. Requests made pursuant to a warrant, subpoena, order, or other legal process issued by a grand jury or judicial or administrative tribunals are presumed to constitute legal authority.

d. Employees will verify the identity of unknown persons requesting access to or disclosure of PHI as follows: to verify the identity of a person requesting PHI in person, the employee will obtain government issued photo identification, to verify the identity of a person requesting PHI over the phone, the employee will ask the caller for the patients' full name and date of birth, to verify the identity of a person requesting PHI by mail, the employee will attempt to match the signature on the letter with the signature maintained in the patient's file.

e. Disclosure of PHI to family or friends: VBJC will generally not disclose PHI to family or friends unless the patient has agreed to such disclosures. If an opportunity to agree or object cannot reasonably be provided in a medical emergency, VBJC will disclose a patient's PHI if, in exercising professional judgment, disclosure is in the best interest of the patient. Employees may discuss the patient's care with the patient, in the presence of friends or family, if the patient either agrees or does not object. Employees may release filled prescriptions, medical supplies, X-rays or other similar forms of PHI to a person involved in the patient's care if the patient has authorized such release or if, in the exercise of professional judgment, the employee reasonably believes it is in the best interest of the patient.

f. Disclosure of PHI via telephone: Employees must be aware of any documented restrictions on the release of patient information and must verify the identity and authority of the individual requesting patient PHI, and use professional judgment and act in the patient's best interest if a concern about the requestor's identity exists. Employees should verify caller's identity via call backs or exchange of information, and request to speak directly with the patient. In the case of a language barrier, ask a third party to obtain oral permission from the patient. Document the patient's oral consent in the medical record, including the name of the third party and the content of the message.

g. Disclosure of PHI via fax: The employee will use the VBJC cover sheet which includes a confidentiality statement instructing anyone who receives the fax in error to destroy the fax and contact the sender, and the cover sheet should not include any type of PHI. Employees will always double check the fax number prior to sending the fax, and routinely monitor fax machines to ensure any incoming fax containing PHI is not left on the machine for an extended period of time.

h. PHI in marketing, fund raising, and research: VBJC does not participate in any fund raising or research. PHI will not be used in any marketing activities for VBJC. If any patients are used for marketing activities, their authorization in writing will be obtained.

i. De-Identified PHI and Limited Data Sets: VBJC may create and use de-identified PHI and limited data sets with out patient authorization. Limited data sets are still protected by HIPPA rules, and may be used for internal VBJC business operations only. De-Identified Information means health information that does not identify any individual who is the subject of the information and for which there is no reasonable basis to believe the information could be used to identify such individual.

j. Personal representatives

1) VBJC will treat a patient's Personal Representative as the patient for the purpose of disclosures of Protected Health Information ("PHI"). The Personal Representative's access to PHI will depend on the scope of their authority. For example, a parent may have different rights with respect to a minor than a health care proxy may have for a patient. Employees must use professional judgment when disclosing information to a patient's Personal Representative and may refuse to share PHI if there is a reasonable belief of domestic violence, abuse, or neglect by the Personal Representative or if disclosure may otherwise endanger the patient.

2) Examples of Personal Representatives include: parents of minors (except for those minors allowed to consent to their own treatment and control their own health information), persons appointed under a health care proxy, or an executor, administrator, or other lawful person who can act on behalf of a deceased individual or his or her estate.

3) Minor's Rights: Patients under the age of 18 are allowed to consent to their own treatment and control their own health information if they are married or have children or have been determined to be emancipated by a court. A pregnant patient under the age of 18 is allowed to consent to her own treatment with respect to her right to make decisions concerning medical, dental, health, and hospital services relating to prenatal care.

10. INDIVIDUAL RIGHTS

a. Right to access/copy PHI: Patients have the right to access or inspect their Protected Health Information ("PHI") contained in the Designated Record Set. Patients also have the right to obtain copies (including electronic) of their PHI contained in their medical record, including imaging studies. It is preferable that patient requests to inspect and/or obtain a copy of PHI be submitted in writing and a copy of the request kept in their medical record.

b. Right to amend PHI: VBJC is committed to maintaining accurate, clear, and complete medical and billing records and to upholding a patient's rights with respect to their health information. To this end, VBJC will permit patients to request in writing that VBJC amend Protected Health Information ("PHI") contained in his or her medical, billing, or other associated records. This right applies only to factual statements contained in the record and not to the provider's observations, inferences, or conclusions. VBJC may deny the request to amend PHI if it determines that the information recorded in the PHI is accurate and complete or was created by another provider.

c. Right to restrict use or disclosure: Patients have the right to request additional restrictions, not otherwise covered by the HIPAA Privacy Policies and Procedures, on the use or disclosure of his or her Protected Health Information ("PHI") for Treatment, Payment, or Health Care Operations or to family or friends involved in the patient's care. VBJC is not required to agree to this restriction, *except when the patient requests such a restriction and pays for the health care item or service in full and out-of-pocket* (i.e., not by their insurer). All patient requests for this restriction must be made in writing and the final bill must be paid in full when the request is received, except in emergency situations.

d. Right to confidential communications**:** At the time of initial registration, the employee will ask the patient for his or her preferred contact information. The employee will document the patient's preferred contact information in the demographics section of the patient's medical record. VBJC permits patients to request confidential or alternative communications with respect to their Protected Health Information ("PHI"). For example, a patient may request that VBJC communicate with them at his or her place of employment rather than his or her place of residence, or at a designated address or phone number. All requests for confidential communications after initial patient registration should be submitted in writing, and the employee must document the date of the request and the alternative communication method or address in the patient's medical record.

e. Right to an accounting of disclosures: VBJC must record certain disclosures of Protected Health Information ("PHI") because patients have a right to receive an accounting of those disclosures. These disclosures include those for for public health activities (e.g., reporting communicable diseases or births/deaths); to report victims of abuse, neglect, and domestic violence; for judicial and administrative proceedings (e.g., pursuant to a valid subpoena); for reports about decedents (e.g., to coroners, medical examiners, and funeral directors); to avert a serious threat to health and safety; for certain specialized government functions (e.g., military and veterans affairs); or for workers compensation purposes. VBJC employees are responsible for recording the necessary disclosures.

Disclosures that do not need to be included: Those for treatment, payment, or business operations; to the patient or their personal representative; in accordance with the patient's written authorization; to family or friends involved in the patient's care or for notification purposes (e.g., to notify a family member of the individual's death); for national security or intelligence purposes; to law enforcement or correctional institutions about an inmate or other person in legal custody; or those made for the creation of De-Identified Information or a Limited Data Set.

f. Right to file a complaint**:** Any individual who has a complaint concerning VBJC's HIPAA Privacy Policies and Procedures or VBJC's compliance with those policies and procedures may file a complaint with VBJC, the Secretary of the U.S. Department of Health and Human Services, or the North Dakota State Department of Health. VBJC will not intimidate, threaten, coerce, discriminate against or retaliate against an individual for filing a complaint, assisting in an investigation, or for opposing any act or practice that the person believes in good faith is unlawful, so long as the manner of such opposition is reasonable and does not involve a disclosure of Protected Health Information ("PHI") in violation of HIPAA. VBJC will not require an individual to waive his or her rights granted in the HIPAA or HITECH acts as a condition to receive treatment, or for VBJC to receive payment.

11. SAFEGUARDS FOR THE PROTECTION OF PHI VBJC will use reasonable and appropriate administrative, technical, and physical safeguards to limit intentional or unintentional uses and disclosures of Protected Health Information (PHI). VBJC will also use these safeguards to protect against the inadvertent disclosure of PHI to persons other than the intended recipient. Employees will only access PHI when there is a legitimate clinical, billing, or business reason to do so. VBJC will monitor all information systems, networks, hardware, and VBJC work sites to ensure compliance with this policy.

a. Administrative safeguards:

- All employees are required to read and sign for their receipt and understanding of the VBJC HIPPA Privacy Policy. This signature form will be retained on file by the privacy manager or where otherwise applicable.

- VBJC will identify employees who need access to PHI to carry out their duties. When possible, restrictions to access only the minimum necessary amount of PHI to perform one's duties will be placed.

- Conversations in which PHI is discussed should be made, to the extent possible, in a manner and location that protects the confidentiality of the information discussed. Conversations with patients or a patient"s family members in public areas should be conducted in a lowered voice, to the extent possible, so that unauthorized individuals cannot overhear the discussion.

- Do not store any VBJC data, including PHI or employee information, on an unencrypted USB or external drive.

b. Physical safeguards:

- Access to areas that contain PHI are monitored and controlled to the reasonable extent possible (e.g., lock doors and file cabinets).

- All documents that contain PHI will be stored and maintained in a manner that minimizes the potential for incidental use or disclosure. Lock drawers and offices when possible.

- All documents containing PHI will be properly disposed of and placed in a locked dedicated container for document shredding.

c. Technical safeguards:

- Store all PHI, Personally Identifiable Information, and VBJC data on the network drive unless absolutely necessary to perform your job duties. If data must be stored on a portable device, that device must be encrypted.

- Emails containing PHI, PII, or other sensitive data must not be sent outside of VBJC unless they are encrypted by using a secure email service. If it is necessary to email PHI, only include the minimum amount of PHI necessary, and only send to the minimum number of recipients necessary, or those who "need to know" to perform their jobs.

- SMS Messaging ("texting") of PHI is not HIPPA compliant. Text messaging encryption programs must be used with any text messages between employees that contains PHI or patient identifiers.

- All laptops and portable devices, used to store Medical Center data, must be encrypted. Do not discard any device containing PHI without first assuring the PHI has been removed or obliterated.

- All employees are responsible for entries and queries under their unique user identity . Users must not share their IDs and/or passwords.

- Employees must log out of databases or electronic health record systems before leaving a work station to prevent inappropriate access to patient information.

- When a patient is left unattended in an exam room, the computer should be locked to prevent someone from gaining access to PHI on the computer. The computer can be locked by using the "Windows" key and the "L" key simultaneously. The computer can then be unlocked with the usual password.

12. WORK FORCE TRAINING

a. All employees are trained on federal and state privacy laws and the VBJC HIPAA Privacy Policy as necessary and appropriate for the employee to carry out their respective job duties. Training of employees will be documented and records maintained by the Privacy Manager for a minimum of six years. When VBJC makes a material change in the HIPAA Privacy Policy that affects the function of an employee, the employee will be trained as necessary and appropriate within a reasonable time after the material change becomes effective.

   1) New staff member training: Training for new employees will occur as soon as reasonably possible.

   2) Recurrent training: Ongoing, targeted training will be provided as necessary to maintain competency regarding privacy policies or as needed for changes in federal or state rules or regulations. Employees will be required to review the VBJC Privacy Policy on an annual basis.

   3) Volunteers and all students exposed to PHI will have a briefing of basic HIPPA policies.

b. The HIPPA training will include a detailed review of the VBJC Privacy Policy and may use other outside training materials as deemed appropriate. Incident specific training will be provided to the affected employee or department after a relevant security or HIPAA related event.

13. BUSINESS ASSOCIATE AGREEMENTS

a. VBJC may engage outside parties to perform functions on VBJC's behalf. In any case where the outside party needs to receive, create, transmit, or maintain Protected Health Information (PHI) on behalf of VBJC, the outside party is known as a Business Associate and a valid Business Associate Agreement must be in place prior to sharing any PHI.

b. A Business Associate Agreement is not required for treatment services provided to the patient (e.g., another physician or a reference laboratory), incidental access to PHI (e.g., janitorial services), and possibly other specific exceptions.

c. Alterations or modifications to our agreements are generally not permitted. The Privacy Manager must approve any vendor requests to alter or modify the Business Associate Agreement prior to execution of the agreement. Only the president or other physician officer of VBJC may sign the Business Associate Agreement for VBJC. All executed Business Association Agreements will be kept of file by the Privacy Manager, and be updated every two years.

14. EMPLOYEE COMPLAINTS

a. Any employee who suspects a security breach should immediately report their concerns to the Privacy Manager or the VBJC President. In an emergency, any VBJC physician can be notified.

b. VBJC will not retaliate against any person who, in good faith, reports a possible security Incident. This will not change their terms of employment.

15. SANCTIONS

a. VBJC will impose appropriate sanctions against Workforce Members who violate HIPAA or the VBJC Privacy Policy. VBJC will consider all relevant factors in determining the nature and severity of the sanction, including but not limited to: the intent of the employee, the severity of the violation, and whether the violation indicated a pattern or practice of improper use or disclosure of PHI.

b. The Privacy Manager along with the VBJC President shall investigate the matter, determine the cause of the violation and take the necessary steps to address the employee non-compliance which may include: a warning, re-training, suspension, or other disciplinary actions, up to and including termination.

c. A record of all sanctions will be kept with the Privacy Manager.

16. BREACH NOTIFICATION

a. VBJC will investigate all Incidents and provide timely notification as necessary and appropriate to: affected individuals, the U.S. Department of Health and Human Services, media outlets, credit reporting agencies, and other federal or state agencies.

b. Upon first knowledge of a potential breach of PHI privacy VBJC will take immediate steps to investigate and contain the Incident and mitigate risk of harm to affected individuals. VBJC may use legal consul and/ or other outside consultants as appropriate.

c. In the event the Incident involves possible criminal activity, such as identity theft or theft of valuable VBJC equipment or proprietary information, the policy manager, after notification of the VBJC president, will file a police report or other notification with the appropriate law enforcement division.

d. For purposes of HIPAA, an Incident is presumed to be a Breach and notification is necessary unless a low probability exists that Protected Health Information (PHI) has been compromised.

e. VBJC may take additional actions as necessary and appropriate to safeguard PHI and to mitigate harm. This includes, but is not limited to: providing identity theft protection services to affected individuals, re-training and educating staff members, implementing controls to prevent further breaches, and implementing disciplinary action up to and including termination of an employee guilty of a breach.