

Title: HIPAA Privacy Policy	Document Reference Number: 8
Site(s): Jupiter Medical Center, Inc.	Type: Organization-wide
Owner: James Mears (Corporate Compliance Officer)	Department(s): Corporate Compliance
Next Review Due Date: 06/09/2025	Date Approved: 06/09/2022

Policy Statement

Jupiter Health, Inc., / Jupiter Medical Center (“JMC”) will use, disclose and release protected health information in accordance with the Privacy and Security Regulations established by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and state law.

Purpose

Provide compliance with state and federal regulations regarding HIPAA and the protection of health information.

Scope

Organization-wide

Definitions

- **Protected Health Information** (“PHI”) - Individually identifiable health information that is transmitted or maintained in any form or medium and that relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to the individual, or the past, present or future payment for the provision of health care by the individual. Information is “individually identifiable” if it either identifies an individual or contains enough specific information to do so. Protected health information includes information of persons living or deceased.
- **Notice of Privacy Practices** (“NPP”) – The Privacy Rule provides that an individual has a right to adequate notice of how JMC may use and disclose PHI about the individual, as well as his or her rights and JMC’s obligations with respect to that information.
- **Use:** The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any member of the workforce of JMC or by a Business Associate (defined below) of JMC.
- **Disclosure:** Means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons not members of the workforce of JMC.
- **Covered Entity:** The entities to which the Privacy Regulations apply including healthcare provider, health plans and healthcare clearing houses.
- **Business Associate** An entity performs or assists in performing a function or activity on behalf of JMC (including claims processing or administration, data analysis, legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.
- **Workforce** - Includes individuals who would be considered part of the workforce under HIPAA such as employees (Team Members), volunteers, trainees, and other persons whose work performance is under the direct control of JMC, whether or not they are paid by JMC.

Policy

1. **Privacy Official and Contact Person**
 - 1.1. The Privacy Officer will be responsible for the development and implementation of policies and procedures relating to privacy.

- 1.2. The Privacy Officer will also serve as the contact person for individuals who have questions, concerns, or complaints about the privacy of their PHI.

2. Workforce Training

- 2.1. It is JMC's policy to train all members of its workforce who have access to PHI on its privacy policies and procedures.
- 2.2. At a minimum, HIPAA training is provided to all new Team Members at orientation and all Team Members participate in mandatory yearly HIPAA training.

3. Safeguards

- 3.1. JMC will establish appropriate administrative, technical, organizational, and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements.
- 3.2. Technical safeguards include among other things, limiting access to information by creating computer firewalls. Firewalls will ensure that only authorized team members will have access to ePHI and that they will have access to only the minimum amount of ePHI necessary to perform their job functions.
- 3.3. Physical safeguards include locking doors or filing cabinets.
- 3.4. Administrative safeguards include performing risk analysis and system audits.
- 3.5. Organizational safeguards include requiring business associate agreements.

4. Privacy Notice

- 4.1. JMC maintains a NPP that describes:
 - 4.1.1. Uses and disclosures of PHI that may be made by JMC;
 - 4.1.2. Individual's rights;
 - 4.1.3. JMC's legal duties with respect to the PHI;
- 4.2. The NPP also provides a description of JMC's complaint procedures, telephone number of the contact person for further information, and the date of the notice.
- 4.3. The NPP is made available to any person who asks for it. JMC also posts the notice in a location where patients can see it and prominently posts on its website.

5. Complaints

Complaints about JMC privacy procedures are handled in accordance with the HIPAA Compliance Policy.

6. Sanctions for Violations of Privacy Policy

Sanctions for using or disclosing PHI in violation of this HIPAA Privacy Policy will be imposed in accordance with the HIPAA Compliance Policy and the Human Resources Corrective Action Policy.

7. Mitigation of Inadvertent Disclosures of Protected Health Information

- 7.1. JMC shall mitigate, to the extent possible, any harmful effects that become known to it because of a use or disclosure of an individual's PHI in violation of the policies and procedures set forth by Jupiter Medical Center.
- 7.2. If a team member becomes aware of a disclosure of protected health information, either by a team member of JMC or another source that is not in compliance with this Policy, they are expected to immediately contact the Privacy Officer so that the appropriate steps to mitigate the harm to the individual can be taken.
- 7.3. Breach Notification shall follow the JMC Breach Notification policy.

8. Non-retaliation:

No team member may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA in accordance with the JMC Non-Retaliation Policy.

9. Permitted Uses and Disclosures:

9.1. **Payment and Health Care Operations** - PHI may be used and disclosed by JMC for the purposes of treatment, payment or operations.

9.1.1. Treatment is the provision, coordination, or management of health care and related services to an individual by one or more health care providers including consultation between providers related to the individual and referral of an individual by one provider to another.

9.1.2. Payment includes activities undertaken to obtain reimbursement for health care. Payment also includes:

9.1.2.1. Eligibility and coverage determinations including coordination of benefits and adjudication or subrogation of health benefit claims;

9.1.2.2. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess loss insurance) and related health care data processing.

9.1.3. Health Care Operations mean any of the following activities:

9.1.3.1. Conducting quality assessment and improvement activities;

9.1.3.2. Reviewing health plan performance;

9.1.3.3. Conducting or arranging for medical review, legal services and auditing functions;

9.1.3.4. Business planning and development; and

9.1.3.5. Business management and general administrative activities.

9.2. **Mandatory Disclosures of PHI: to Individual and Department of Health and Human Services (DHHS)** - PHI must be disclosed as required by HIPAA when:

9.2.1. Disclosure is to the individual who is the subject of the information; and

9.2.2. Disclosure is made to DHHS for purposes of enforcement of HIPAA.

9.3. **Permissive Disclosures of PHI: for Legal and Public Policy Purposes which may include:**

9.3.1. About victims-of abuse, neglect or domestic violence;

9.3.2. For judicial and administrative proceedings;

9.3.3. For law enforcement purposes;

9.3.4. For public health activities;

9.3.5. For health oversight activities;

9.3.6. About decedents to funeral directors, coroners or medical examiners as authorized by law;

9.3.7. To facilitate cadaver organ, eye or tissue donation;

9.3.8. For certain limited research purposes;

9.3.9. To avert a serious threat to public health or safety;

9.3.10. For specialized government functions; and

9.3.11. That relate to workers' compensation programs.

9.4. **Disclosures of PHI Pursuant to an Authorization**

9.4.1. PHI may be disclosed for any purpose if an authorization that satisfies all of HIPAA's requirements for a valid authorization is provided by the patient.

9.4.2. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

9.5. Complying With the "Minimum-Necessary" Standard

- 9.5.1. HIPAA requires that when PHI is used or disclosed, the amount disclosed generally must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure.
- 9.5.2. The "minimum-necessary" standard does not apply to any of the following:
 - 9.5.2.1. Uses or disclosures made to the individual;
 - 9.5.2.2. Uses or disclosures made pursuant to a valid authorization;
 - 9.5.2.3. Disclosures made to the DHHS for complaint investigation;
 - 9.5.2.4. Uses or disclosures made for Treatment purposes;
 - 9.5.2.5. Uses or disclosures required by law; and
 - 9.5.2.6. Uses or disclosures required to comply with HIPAA.
- 9.5.3. When making disclosures of PHI to a Covered Entity, Business Associate or internal/external auditing purposes, only the minimum necessary amount of information will be disclosed.

9.6. Disclosures of PHI to Business Associates

- 9.6.1. JMC workforce members may disclose PHI to JMC's business associates and allow business associates to create or receive PHI on its behalf. However, prior to doing so, JMC must first obtain assurances from the business associate that it will appropriately safeguard the information.
- 9.6.2. Before sharing PHI with outside consultants or contractors who meet the definition of a "business associate," employees must verify that a business associate agreement is in place. Business Associate Agreements ("BAA") are put in place in accordance with the JMC HIPAA Business Associate Policy and BAA Decision Tree.

9.7. Disclosures of De-Identified Information - JMC may use and disclose de-identified information.

- 9.7.1. De-identified information is health information that does not identify an individual to the extent that there is no reasonable basis to believe that the information can be used to identify an individual.
- 9.7.2. There are two ways a covered entity can determine that information is de-identified: either by professional statistical analysis, or by removal of specific identifiers of the individual, the individual's relatives, household members and employer so that any remaining information cannot be used to identify the individual.

10. Policies on Individual Rights

10.1. Access to Protected Health Information and Requests for Amendment

- 10.1.1. HIPAA gives individuals the right to access and obtain copies of their PHI that JMC or its business associates maintains in designated record sets.
- 10.1.2. HIPAA also provides that individuals may request to have their PHI amended.
- 10.1.3. JMC will provide access to PHI and it will consider requests for amendment that are submitted in writing by individuals.

10.2. Accounting

- 10.2.1. An individual has the right to obtain an accounting of certain disclosures of his or her own PHI.
- 10.2.2. This right to an accounting extends to disclosures made in the last six years, other than disclosures:
 - 10.2.2.1. Carry out treatment, payment or health care operations;
 - 10.2.2.2. To individuals about their own PHI;
 - 10.2.2.3. Incident to an otherwise permitted use or disclosure or pursuant to an authorization;
 - 10.2.2.4. For purposes of creation of a facility directory or to persons involved in the patient's care or other notification purposes;
 - 10.2.2.5. As part of a limited data set; or

HIPAA Privacy Policy Continued

- 10.2.2.6. For other national security or law enforcement purposes.
- 10.2.3. JMC shall respond to an accounting request within 60 days. If JMC is unable to provide the accounting within 60 days, it may extend the period by 30 days, provided that it gives the patient notice (including the reason for the delay and the date the information will be provided) within the original 60-day period.
- 10.2.4. The accounting must include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure (or a copy of the written request for disclosure, if any).
- 10.2.5. The first accounting in any 12-month period shall be provided free of charge.
- 10.2.6. The Medical Records Department may impose reasonable production and mailing costs for subsequent accountings.
- 10.3. Requests for Alternative Communication Means or Locations
 - 10.3.1. Patients may request to receive communications regarding their PHI by alternative means or at alternative locations. For example, individuals may ask to be called only at work rather than at home.
 - 10.3.2. Such requests may be honored if, in the sole discretion of JMC, the requests are reasonable.
 - 10.3.3. JMC shall accommodate such a request if the participant clearly provides information that the disclosure of all or part of that information could endanger the participant.
- 10.4. Requests for Restrictions on Uses and Disclosures of Protected Health Information
 - 10.4.1. A patient may request restrictions on the use and disclosure of the patient's PHI.
 - 10.4.2. It is JMC's policy to attempt to honor such requests if, in the sole discretion of JMC, the requests are reasonable.

Related Documents

- [HIPAA Compliance Policy](#)
- [HIPAA Compliance Procedure](#)
- [HIPAA Business Associates](#)
- [HIPAA Breach Notification Policy](#)
- [Acceptable Use Policy](#)
- [Data Encryption Policy](#)
- [Corrective Action - Human Resources](#)
- [JMC Non-Retaliation Policy](#)
- [Shredding Documents](#)
- [JMC HIPAA Notice of Privacy Practices Brochure](#)
- [JMC HIPAA Notice Of Privacy Practices Poster](#)

References

HIPAA Privacy Rule 45 CFR § 164.500

**Approved by: Policy Committee, Steven Seeley
(VP Chief Operating Officer)**

Approve Date: 06/09/2022