EPIONE HEALING, LLC
DBA VIRTUS SPORT AND EXTREMITY

HIPAA PRIVACY & SECURITY POLICY

VIRTUS

SPORT & EXTREMITY

August 2023

Table of Contents

HIPPA Privacy & Security Policy

HIPAA Privacy & Security Policy

Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations restrict Epione Healing, LLC ("Epione", "Company") abilities to use and disclose protected health information (PHI).

Protected Health Information. Protected health information means information that is created or received by the Company and relates to the past, present, or future physical or mental health condition of a Patient; 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. Protected health information includes information of persons living or deceased.

Some examples of PHI are:

- Patient's medical record number
- Patient's demographic information (e.g. address, telephone number)
- Information doctors, nurses and other health care providers put in a patient's medical record
- Images of the patient
- Conversations a provider has about a patient's care or treatment with nurses and others
- Information about a patient in a provider's computer system or a health insurer's computer system
- Billing information about a patient at our clinic
- Any health information that can lead to the identity of an individual or the contents of the information can be used to make a reasonable assumption as to the identity of the individual

It is the Company's policy to comply fully with HIPAA's requirements. To that end, all staff members who have access to PHI must comply with this HIPAA Privacy and Security Policy. For purposes of this Plan and the Company's use and disclosure procedures, the workforce includes individuals who would be considered part of the workforce under HIPAA such as employees, volunteers, interns, and other persons whose work performance is under the direct control of Epione, whether or not they are paid by Epione. The term "employee" or "staff member" includes all of these types of workers.

No third-party rights (including but not limited to rights of participants, beneficiaries, covered dependents, or business associates) are intended to be created by this Plan. Epione reserves the right to amend or change this Plan at any time (and even retroactively) without notice.

All staff members must comply with all applicable HIPAA privacy and information security policies. If after an investigation you are found to have violated the organization's HIPAA privacy and information security policies then you will be subject to disciplinary action up to termination or legal ramifications if the infraction requires it.

SECTION 1: Responsibilities as a Covered Entity

I. Privacy Officer

Dr. Molly Sparks, D.C. will be the HIPAA Privacy Officer for Epione Healing, LLC. The Privacy Officer will be responsible for the development and implementation of policies and procedures relating to privacy, including but not limited to this Privacy Policy and the Company's use and disclosure procedures. The Privacy Officer will also serve as the contact person for patient who have questions, concerns, or complaints about the privacy of their PHI. The Privacy Officer can be reached at drsparks@virtusclinics.com and 206-960-3448.

In the event of a security incident results in a wrongful disclosure of PHI, the Privacy Officer will take appropriate actions to prevent further inappropriate disclosures. In addition, outside legal counsel may be consulted as part of the review team to assist in the review and investigation of privacy incidents when required. If the Privacy Officer has not resolved the incident, the Privacy Officer shall involve anyone determined to be necessary to assist in the resolution of the incident. If patients need to be notified of any lost/stolen PHI, the Privacy Officer will send PHI Theft/Loss Disclosure Letters to all possible affected individuals.

II. Workforce Training

It is the Company's policy to train all members of its workforce who have access to PHI on its privacy policies and procedures. All staff members receive HIPAA training. Whenever a privacy incident has occurred, the Privacy Officer in collaboration with management will evaluate the occurrence to determine whether additional staff training is in order. Depending upon the situation, the Privacy Officer may determine that all staff should receive training that is specific to the privacy incident. The Privacy Officer will review any privacy training developed as part of a privacy incident resolution to ensure the materials adequately address the circumstances regarding the privacy incident and reinforce the Company's privacy policies and procedures.

III. Safeguards

The Company has established technical and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Technical safeguards include limiting access to information by creating computer firewalls. Physical safeguards include locking doors or filing cabinets. Additionally all staff members can only access PHI by using their own login information.

Firewalls ensure that only authorized employees will have access to PHI, that they will have access to only the minimum amount of PHI necessary for their job functions, and that they will not further use or disclose PHI in violation of HIPAA's privacy rules. Data is stored on a central secure sever in a locked room and is routinely back up using industry standards.

IV. Privacy Notice

The Privacy Officer is responsible for developing and maintaining a notice of the Company's privacy practices that describes:

- the uses and disclosures of PHI that may be made by the Company;
- the individual's rights; and
- the Company's legal duties with respect to the PHI.

The privacy notice will inform patients that the Company will have access to PHI. The privacy notice will also provide a description of the Company's complaint procedures, the name and telephone number of the contact person for further information, and the date of the notice.

The notice of privacy practices will be individually delivered to all patients:

- on an ongoing basis, at the time of an individual's treatment and consent; and
- within 60 days after a material change to the notice.

The Company will also provide notice of availability of the privacy notice at least once every three years.

V. Complaints

The Privacy Officer will be the Company's contact person for receiving complaints. The Privacy Officer is responsible for creating a process for individuals to lodge complaints about the Company's privacy procedures and for creating a system for handling such complaints.

VI. Sanctions for Violations of Privacy Policy

Sanctions for using or disclosing PHI in violation of this HIPAA Privacy Plan will be imposed in accordance up to and including termination.

VII. Mitigation of Inadvertent Disclosures of Protected Health Information

Epione shall mitigate, to the extent possible, any harmful effects that become known to it because of a use or disclosure of a patient's PHI in violation of the policies and procedures set forth in this Plan. As a result, if an employee becomes aware of a disclosure of PHI, either by a staff member of the Company or an outside consultant/contractor that is not in compliance with this Policy, immediately contact the Privacy Officer so that the appropriate steps to mitigate the harm to the participant can be taken.

VIII. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy

No employee 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.

No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment or payment.

IX. Policy Document

This Policy document includes provisions to describe the permitted and required uses and disclosures of PHI by Epione. Specifically, the Plan requires Epione to:

- not use or further disclose PHI other than as permitted by the Plan documents or as required by law;
- ensure that any agents or subcontractors to whom it provides PHI received from the Company agree to the same restrictions and conditions that apply to Epione;
- report to the Privacy Officer any use or disclosure of the information that is inconsistent with the permitted uses or disclosures;
- make PHI available to patients, and, upon request, provide them with an accounting of PHI disclosures; and
- make the Company's internal practices and records relating to the use and disclosure of PHI received by the Company available to the Department of Health and Human Services (HHS) upon request.

X. Documentation

The Company's privacy policies and procedures shall be documented and maintained for at least six years. Policies and procedures must be changed as necessary or appropriate to comply with changes in the law, standards, requirements and implementation specifications (including changes and modifications in regulations). Any changes to policies or procedures must be promptly documented.

If a change in law impacts the privacy notice, the privacy policy must promptly be revised and made available. Such change is effective only with respect to PHI created or received after the effective date of the notice.

Epione shall document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to an individual's privacy rights.

The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form.

Incident Report

The Company has developed an Incident Report form. This form is used to document reports of privacy

breaches that have been referred to the Privacy Officer from staff members who have reviewed or received the suspected incident.

After receiving the Incident Report form from staff members, the Privacy Officer classifies the incident and its severity and analyzes the situation. Documentation shall be retained by the Company for a minimum of six years from the date of the reported incident.

If the Privacy Officer is able to resolve the incident, the Privacy Officer shall also document the actions taken to resolve the issue in the Incident Report form.

XI. Electronic Health Records

Just like paper records, Electronic Health Records must comply with HIPAA, and other state and federal laws. Unlike paper records, electronic health records can be encrypted - using technology that makes them unreadable to anyone other than an authorized user - and security access parameters are set so that only authorized individuals can view them. Further, EHRs offer the added security of an electronic tracking system that provides an accounting history of when records have been accessed and who accessed them.

XII. Access Authorization

Epione will grant access to PHI based on their job functions and responsibilities.

The Privacy Officer is responsible for the determination of which individuals require access to PHI and what level of access they require. The Company will keep a record of authorized users and the rights that they have been granted with respect to PHI.

A summary of user rights can be found in the table below.

Job Title	**User Rights**
Doctors	Full Access to PHI – including (but not limited to) construction of chart notes, diagnosis, billable charges, modify patient information.
Office Manager	Appointment Scheduling View Patient Information Daily Appointment Reports Faxing Medical Records
Rehab Specialists	No Electronic Health Record Access View Patient First and Last Names Only Appointment Scheduling

SECTION 2: Use and Disclosure of PHI

I. Use and Disclosure Defined

The Company will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

- *Use.* The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any person working for or within the Company, or by a Business Associate of the Company.

- *Disclosure.* For information that is protected health information, disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons not employed by or working within Epione with a business need to know PHI.

II. Access to PHI Is Limited to Certain Employees

All staff who perform patient functions directly on behalf of the Company will have access to PHI as determined by their job description.

These employees with access may use and disclose PHI as required under HIPAA but the PHI disclosed must be limited to the minimum amount necessary to perform the job function. Employees with access may not disclose PHI unless an approved authorization is in place or the disclosure otherwise is in compliance with this Plan and the use and disclosure procedures of HIPAA.

Staff members may not access either through Company's information systems or the patient medical record the medical and/or demographic information for themselves, family members, friends, staff members or other individuals for personal or other non-work related purposes, even if written or oral participant authorization has been given.

III. Disclosures of PHI Pursuant to an Authorization

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

IV. Permissive Disclosures of PHI: for Legal and Public Policy Purposes

PHI may be disclosed in the following situations without a patient's authorization, when specific requirements are satisfied. The Company's use and disclosure procedures describe specific requirements that must be met before these types of disclosures may be made.

Permitted are disclosures:

- about victims-of abuse, neglect or domestic violence;
- for judicial and administrative proceedings;
- for law enforcement purposes;
- for public health activities;
- for health oversight activities;
- for certain limited research purposes;
- to avert a serious threat to health or safety;
- for specialized government functions; and
- that relate to workers' compensation programs.

V. Complying With the "Minimum-Necessary" Standard

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.

The "minimum-necessary" standard does not apply to any of the following:

- uses or disclosures made to the individual;
- uses or disclosures made pursuant to a valid authorization;
- disclosures made to the Department of Labor;
- uses or disclosures required by law; and
- uses or disclosures required to comply with HIPAA.

Minimum Necessary When Disclosing PHI. For making disclosures of PHI to any business associate or providers, or internal/external auditing purposes, only the minimum necessary amount of information will be disclosed.

All other disclosures must be reviewed on an individual basis with the Privacy Officer to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

Minimum Necessary When Requesting PHI. For making *requests* for disclosure of PHI from business associates, providers or patients for purposes of claims payment/adjudication or internal/external auditing purposes, only the minimum necessary amount of information will be requested.

All other requests must be reviewed on an individual basis with the Privacy Officer to ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

VI. Disclosures of PHI to Business Associates

With the approval of the Privacy Officer and in compliance with HIPAA, employees may disclose PHI to the Company's business associates and allow the Company's business associates to create or receive PHI on its behalf. However, prior to doing so, the Company must first obtain assurances from the business associate that it will appropriately safeguard the information. Before sharing PHI with outside consultants or contractors who meet the definition of a "business associate," employees must contact the Privacy Officer and verify that a business associate contract is in place.

Business Associate is an entity that:

- performs or assists in performing a Company function or activity involving the use and disclosure of protected health information (including claims processing or administration, data analysis, underwriting, etc.); or

- provides 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.

Examples of Business Associates are:

- A third party administrator that assists the Company with claims processing.
- A CPA firm whose accounting services to a health care provider involves access to protected health information.
- An attorney whose legal services involve access to protected health information.
- A consultant that performs utilization reviews for the Company.
- A health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of the Company and forwards the processed transaction to a payer.

VII. Disclosures of De-Identified Information

The Company may freely use and disclose de-identified information. De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. There are two ways a covered entity can determine that information is de-identified: either by professional statistical analysis, or by removing 18 specific identifiers.

18 specific elements listed below - relating to the patient - must be removed, and you must ascertain there is no other available information that could be used alone or in combination to identify an individual.

1. Names
2. Geographic subdivisions smaller than a state
3. All elements of dates (except year) related to an individual - including dates of admission, discharge, birth, death - and for persons >89 y.o., the year of birth cannot be used.
4. Telephone numbers
5. FAX numbers
6. Electronic mail addresses
7. Social Security Number
8. Medical Record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers including license plates
13. Device identifiers and serial numbers
14. Web URLs
15. Internet protocol addresses
16. Biometric identifiers, including finger and voice prints
17. Full face photos, and comparable images
18. Any unique identifying number, characteristic or code

A person with appropriate expertise must determine that the risk is very small that the information could be used alone or in combination with other reasonably available information by an anticipated recipient to identify the individual. AND this person must document the methods and justification for this determination.

VIII. Removing PHI from Company Premises

Employees only work onsite and are not permitted to access or remove PHI from Epione's premise. The following safeguards are required of doctors when working from a non-Epione location:

- When outside the clinic, only work on health information in a **secure private environment.**
- Keep the information with you **at all times** while in transit.
- Do not permit others to have access to the information.
- Don't save patient information to your home computer.
- Do not print records of any type.
- Do not record login information on or near the computer.
- Return all information the next business day or as soon as required.

The Privacy Officer will immediately investigate any incident that involves the loss or theft of PHI that was taken off-site.

IX. Faxing PHI

Each fax should be accompanied by an Epione fax cover sheet. Faxing of highly confidential information is not recommended. Faxing of highly confidential information is only permitted if the sender first calls the recipient and confirms that the recipient or his/her designee can be waiting at the fax machine, and then, the recipient or his/her designee waits at the fax machine to receive the fax and then calls the sender to confirm receipt of the document. Both the sender and the recipient must be attentive to the sensitive nature of highly confidential information.

If the fax was transmitted to the wrong recipient, in all cases follow these steps:

Fax a request to the incorrect fax number explaining that the information has been misdirected, and ask that the materials be returned or destroyed. Document the incident on an Incident Report Form and notify the HIPAA Privacy Officer at drsparks@virtusclinics.com *[206-960-3448]*. Verify the fax number with the recipient before attempting to fax the information again.

SECTION 3: Participant Individual Rights

I. Access to Protected Health Information and Requests for Amendment

HIPAA gives patients the right to access and obtain copies of their PHI that the Company or its business associates maintains. HIPAA also provides that patients may request to have their PHI amended. The Company will provide access to PHI and it will consider requests for amendment that are submitted in writing by patients.

II. Accounting

An individual has the right to obtain an accounting of certain disclosures of his or her own PHI. This right to an accounting extends to disclosures made in the last six years, other than disclosures:

• to carry out treatment, payment or health care operations;

• to individuals about their own PHI;

• incident to an otherwise permitted use or disclosure or pursuant to an authorization;

• for purposes of creation of a facility directory or to persons involved in the participant's care or other notification purposes;

• as part of a limited data set; or

• for other national security or law enforcement purposes.

The Company shall respond to an accounting request within 60 days. If the Company 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.

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).

The first accounting in any 12-month period shall be provided free of charge. The Privacy Officer may impose reasonable production and mailing costs for subsequent accountings. The Privacy Officer is responsible for responding to a request for Accounting.

III. Requests for Restrictions on Uses and Disclosures of Protected Health Information

A patient may request restrictions on the use and disclosure of the patient's PHI. It is the Company's policy to attempt to honor such requests if, in the sole discretion of the Company, the requests are reasonable. The Privacy Officer is charged with responsibility for processing requests for restrictions.

IV. When a Patient Requests a Copy of his/her Record

A participant can request a copy of his/her medical record by placing a request with the front desk. The front desk staff in collaboration with the Privacy Officer will process and respond to such request.

V. Patient Request for copy of Clinic Notes or Labs while Checking out After an Appointment

It's okay to provide a patient with a copy of a clinic note or labs that are maintained in their files. It is recommended that you follow the best practice of stamping or writing "Patient Copy" on **each** page.

VI. Acceptable Methods of Verification of Identity for Release of Personal Health Information (PHI):

When the Requestor is the Patient

The Company will take reasonable steps and exercise professional judgment to verify the identity of the individual making a request for access to his/her own PHI.

a. **If the request is made in person**, verification of identity may be accomplished by asking for photo identification (such as a driver's license). A copy of the I.D. must be attached to the request and placed in the patient record.

b. **If the request is made over the telephone**, verification will be accomplished by requesting identifying information such as social security number, birth date, and medical record number and confirming that this information matches what is in the participant's record. Or, verification will occur through a callback process using phone numbers documented in the participant record to validate the caller's identity.

c. **If the request is made in writing,** verification will be accomplished by requesting a photocopy of photo identification if a photocopy of the ID is not available, the signature on the written request must be compared with the signature in the participant record. In addition, Epione will need to verify the validity of the written request by contacting the participant by telephone.

V1II. When the requestor is the Patients Legally Authorized Representative

Verification of identity will be accomplished by asking for a valid photo identification (such as driver's license) if the request is made in person. Once identity is established, authority in such situations may be determined by confirming the person is named in the medical record or in the patients profile as the patients legally authorized representative. Or, if there is no person listed in the medical record as the patients legally authorized representative, authority may be established by the person presenting an original of a valid power of attorney for health care or a copy of a court order appointing the person guardian of the participant and a valid photo I.D. A copy of the I.D. and legal notice must be attached to the request and placed in the patients record.

IX. Other Methods

The Company may use any other method of verification that, in the Company's discretion, is reasonably calculated to verify the identity of the person making the request. Some acceptable means of verification include, but are not limited to:

a. Requesting to see a photo ID
b. Requesting a copy of a power of attorney
c. Confirming personal information with the requestor such as date of birth, policy number or social security number

PHI Breach Reporting

The purpose of this section is to address the Company's privacy requirements for reporting, documenting, and investigating a known or suspected action or adverse event resulting from unauthorized use or disclosure of individually identifiable health information.

A privacy breach is an adverse event or action that is unplanned, unusual, and unwanted that happens as a result of non-compliance with the privacy policies and procedures of the Company. A privacy breach must pertain to the unauthorized use or disclosure of health information, including 'accidental disclosures' such as misdirected e-mails or faxes.

The Privacy Officer shall immediately investigate and attempt to resolve all reported suspected privacy breaches.

Employees are required to verbally report to the Privacy Officer any event or circumstance that is believed to be an inappropriate use or disclosure of a participant PHI within 24 hours of the incident. The Privacy Officer will determine whether the suspected incident warrants further investigation. In all cases and Incident Report must be filled out and submitted to the appropriate reviewer.

The Privacy Officer will document all privacy incidents and corrective actions taken. Documentation shall include a description of corrective actions, if any are necessary, or explanation of why corrective actions are not needed, and any mitigation undertaken for each specific privacy incident. All documentation of a privacy breach shall be maintained with the Privacy Officer and shall be retained for at least six years from the date of the investigation. Such documentation is not considered part of the patient's health record.

If the patient is not aware of a privacy incident, the Privacy Officer shall investigate the incident thoroughly before determining whether the patient should be informed. If the patient is aware of a privacy incident, the Privacy Officer shall contact the patient promptly upon receiving notice of the incident. The method of contact is at the discretion of the Privacy Officer, but resulting communications with the patient must be documented in the incident report. In addition, any privacy incident that includes a disclosure for which an accounting is required must be documented and entered into accounting.

Employees who fail to report known PHI/security incidents, or fail to report them promptly, may be subject to disciplinary action up to termination.

I. Breach Notification Requirements

Following a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals if necessary and in certain circumstances, to the media. In addition, business associates must notify covered entities that a breach has occurred.

- *Individual Notice*

Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information. Covered entities must provide this individual notice in written form by

first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site or by providing the notice in major print or broadcast media where the affected individuals likely reside. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written, telephone, or other means.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity. Additionally, for substitute notice provided via web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact the covered entity to determine if their protected health information was involved in the breach.

- *Media Notice*

Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

- *Notice to the Secretary*

In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred.

- *Notification by a Business Associate*

If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any information required to be provided by the covered entity in its notification to affected individuals.

II. Complaint/Concerns Reporting

Concerns about the Company's privacy practices may arise in a variety of contexts and may be received by many different persons at the Company. It is important that the Company responds to concerns and complaints in a timely manner. When a staff member hears or receives a complaint/concern, he/she should ask the complainant whether or not the complainant wishes to file a formal complaint and offer to assist the complainant with the form. Even if the person does not wish to file a complaint or provide identifying information, the staff member should proceed with the procedures outlined below.

Filing a Complaint

a. **Patient's** complaints of alleged privacy rights violations may be forwarded through multiple channels, such as telephone calls, letter via mail/email, in person. If these complaints are received by a staff member the person receiving the complaint will:

- Complete the Privacy complaint form and immediately forward to the Privacy Officer, along with other supporting documentation.

b. **Staff Members** – Call the Privacy Officer at 206-960-3448. Staff members may also complete the Privacy Complaint Form and forward to the Privacy Officer. Upon receipt of a complaint, the Privacy Officer will initiate primary investigation.

- **Initial review** – All complaints will be initially reviewed by the Privacy Officer or his/her designee to determine if the complaint alleges a violation of established policies and procedures or other known regulations regarding the protection of individually identifiable health information. If there is no legitimate allegation, the Privacy Officer will, when possible, contact the Complainant by letter and inform him/her of this finding within 60 days. All documentation will be maintained as prescribed in this policy.
- **Complaints requiring further review** – If there is a legitimate allegation, the Privacy Officer or his/her designee will conduct a detailed investigation by contacting employees as needed, reviewing Company's polies, and utilizing other Company resources as needed. Upon conclusion of the investigation, the Privacy Officer will, when possible, contact the Complainant by letter and inform him/her of the finding within 60 days.

c. **60-day time frame –** In the event that this 60-day period cannot be met, the Privacy Officer shall, when possible, communicate this determination to the Complainant in writing and include an estimated timeframe for completion of the investigation.

d. **Outcome of Investigation -** The purpose of the investigation is to determine the compliance of the Company's policies and procedures implementing the privacy standards mandated by HIPAA. The Company will mitigate, to the extent practicable, any harmful effect that is known of a use or disclosure of PHI in violation of the Company's policies and procedures or HIPAA's privacy requirements by the Company or any of its Business Associates.

e. **Documentation -** All complaints sent to the Privacy Officer shall be documented in a format that includes all of the information contained on the Privacy Complaint Form. The Privacy Officer will maintain all completed complaints' documentation for six (6) years from the initial date of the complaint.

III. Non-Retaliation

The Company shall not intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any person who has reported a privacy incident.

ATTACHMENTS

EPIONE HEALING
NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

Our pledge to protect your privacy
Epione is required by law to maintain the privacy and security of your protected health information. Your care and treatment is recorded in a medical record. So that we can best meet your medical needs, we may share your medical record with the providers involved in your care. We share your information only to the extent necessary to collect payment for the services we provide, to conduct our business operations, and to comply with the laws that govern health care. We will not use or disclose your information for any other purpose unless you tell us we can in writing. If you tell us we can, you may change your mind at any time. Let us know in writing if you change your mind. We will also let you know promptly if a breach occurs that may have compromised the privacy or security of your information.

Patient's Rights – When it comes to your health information, you have certain rights.
This section explains your rights and some of our responsibilities to help you. To exercise any of your rights, please contact our office directly either by phone or mail at the contact information at the end of this Notice. You will not be retaliated against for filing a complaint.

As a patient, you have the right:
- to request to inspect and obtain a copy of your electronic or paper medical records and other health information we have about you
- to request to add an addendum to or correct your medical record;
- to request an accounting of Epione's disclosures of your medical information;
- to request restrictions on certain uses or disclosures of your medical information;
- to request that we communicate with you in a certain way or at a certain location (for example, home or office phone) or to send mail to a different address.
- to file a complaint if you feel your rights are violated[1]
- to obtain a copy of this privacy notice at any time

We may use and disclose medical information about you for the following purposes:
- to provide you with medical treatment and services;
- to bill and receive payment for the treatment and services you receive;
- for functions necessary to run Epione Healing and assure that our patients receive quality care;
- and as required or permitted by law.

[1] [1] You can also file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights by sending a letter to 200 Independence Avenue, S.W., Washington D.C. 20201, calling 1-877-696-6775, or visiting www.hhs.gov/ocr/privacy/hipaa/complaints/

There are additional situations where we may disclose medical information about you without your authorization, such as:

- for workers' compensation or similar programs;
- for public health activities (e.g., reporting abuse or reactions to medications);
- to a health oversight agency, such as the Washington Department of Health;
- in response to a court or administrative order, subpoena, warrant or similar process;
- to law enforcement officials in certain limited circumstances;

Our Notice may be revised or updated from time to time, and the changes will apply to all information we have about you. The new notice will be available upon request.

How to contact Epione Healing to file a complaint or exercise any of your other rights under this Notice. Please contract us directly by phone during normal hours of operation or by mail.

By phone: (425)-457-6532

By Mail:
Epione Healing d/b/a Virtus Sport and Extremtiy
Attn: Dr. Molly Sparks, Privacy Officer
126th Central Way
Kirkland, WA 98033

For further information about our Notice of Privacy Practices, please contact Epione's Privacy Officer at: (206)-960-3448.

EPIONE HEALING
Accounting of Non-Authorized Use or Disclosure Request Form

The HIPAA Privacy Regulations allow an individual to request an accounting of certain disclosures of his/her Protected Health Information (PHI). Epione Healing, LLC may disclose your PHI for treatment, payment, health care operations, and as required or permitted by the HIPAA Privacy Regulation or other state or federal laws. Our Privacy Notice informs you that these disclosures may occur without your consent at the time they are made.

You can request an accounting of certain disclosures only about yourself, unless you are authorized to obtain information about another individual. Please complete this form to request a disclosure and return it to EPIONE HEALING, ATTN: Privacy Officer, 126th Central Way Kirkland, WA 98033

INDIVIDUAL'S INFORMATION		
Name:	Medical Record # or ID#:	
Birthdate:	Contact Phone Number:	Request Date:
Current Address (No., street, city, state, zip):		

DISCLOSURE REQUESTED

I request that Epione Healing provide me with an accounting of any and all applicable "non-authorized" uses and disclosures of my protected health information (PHI) between _____ (beginning date) and _____(ending date).

I would like to limit this request for accounting to include disclosures only pertaining to:

_____

I want the accounting of disclosures in the following form: *(check one)*

□ Mail to my current address on file: _____

□ I want to pick up the accounting.
Please call me at the following telephone number when it is ready: _____

I understand that I may be charged for this information if I have previously requested this information within the last 12 months. There will be a fee for any additional accountings within the same 12 month period. I will be informed of the cost for such additional accounting in advance and will be provided with the opportunity to withdraw or modify the request in order to reduce or avoid the fee. I understand that Epione Healing must give me the accounting of disclosures within 60 days, or must tell me that it needs up to 30 extra days to prepare it.

I understand that Epione Healing does not have to tell me about the following types of disclosures:

1. Disclosures made as part of a limited data set for purposes of research, public health, or health care operations, as permitted by federal law.
2. Disclosures made for purposes of treatment, payment and health care operations.
3. Disclosures made to me or disclosures consented to or authorized by me.
4. Disclosures made to persons involved in my care.
5. Disclosures made for national security or intelligence purposes.
6. Disclosures made to correctional institutions or law enforcement officials, under certain circumstances.
7. Disclosures made incident to a use or disclosure otherwise permitted or required by law.

ACKNOWLEDGEMENT
Please sign and date:

By: _____ _____
Patient's Name (Print) Patient's Signature

If you are not the patient, please complete, sign and date below. Check the box that describes your relationship to the patient. Please attach proof or your relationship to the patient (e.g. Power of Attorney, legal guardian)

Comments of Epione Provider:

By: _____ _____
Name (Print) Signature

□Parent of Minor Child □Legal Guardian □Power of Attorney □Executor □Other

Request Determination

This Section for Company Use Only

Privacy Officer Action/Comments:
Action must be taken within 60 days of the receipt of the request

Request has been: □ Accepted □ Denied (If denied, please explain):

Disclosure Request has been reviewed by the following Provider(s):

Date	**Please Print Name**	**Signature of Provider**
Date	**Please Print Name**	**Signature of Provider**

Notification was sent to the Patient on:

Date

Send a copy of completed form to individual. Send original to Medical Records to place in individuals Medical Records file. Date copy sent: Copy sent by (print name:

EPIONE HEALING
INCIDENT REPORT
FORM

Date of Incident: _____ Time of Incident: _____ am/pm

Location: _____

Person(s) Involved Name: _____ If Patient MR#_____
(Circle one) Patient Staff Volunteer Other_____

Witness(es)_____

NATURE OF INCIDENT (check all that apply):

- HIPAA Violation/Breach of Confidentiality
- Complaint/Grievance
- Other _____

DETAILS OF INCIDENT (include all known facts, persons involved, statements, cause, witnesses, time, location)

_____
_____
_____
_____
_____

RESOLUTION (if applicable)

_____
_____
_____
_____

REPORTING

Note: Incidents must be reported within 24 hours of occurrence to the Privacy Officer. A copy of this form must be given to the Privacy Officer

Incident Reported to: _____ Title:_____
Date: _____

Report completed by: _____Title: _____
Date: _____ Contact number: _____

OFFICIAL REVIEW

Incident reviewed by: Privacy Officer

If applicable, Severity of HIPAA Privacy Incident:

□ Severe Press may be involved. Affects participant and/or public, business associates, and/or state and/or local government.

□ Moderate Press involvement unlikely. Affects participant and/or business associates.

□ Low No affect outside of company. Company able to resolve

COMMENTS BY REVIEWER(S):

RESOLUTION/CORRECTIVE ACTION:

□ Staff Training Needed □ Procedures to be Reviewed □ Employee Sanctions
□ Inform Patient □ Record disclosure in accounting of disclosures log with Privacy Officer

o No further action required, ok to file

Signature:

Title:

Date: _____