HIPAA PRIVACY POLICIES AND PROCEDURES
OF
ON LOCATION, IV HYDRATION, LLC
(the "Company")

Adopted May 8, 2023

HIPAA Privacy Policy and Procedure No. 1
Privacy Officer and Security Officer

Purpose

This policy is designed to ensure the establishment of a Privacy Office for the purpose of overseeing Company obligations to maintain the privacy of protected health information ("PHI") consistent with state and federal privacy laws in accordance with 45 CFR § 164.530.

Policy

Company has designated a Privacy Officer and a Security Officer.

Definitions

Capitalized terms used but not defined herein shall have the meanings given to them by the Health Insurance Portability and Accountability Act ("HIPAA") and/or the implementing regulations thereof (the "HIPAA Rules").

I. Privacy Officer

Purpose: The Privacy Officer will oversee the implementation and enforcement of these HIPAA Privacy Policies. The Privacy Officer is responsible for all obligations specified in these policies as being an action required to be performed by, or supervised by, the Privacy Officer. The Privacy Officer may designate one or more authorized representatives who may assist the Privacy Officer in implementing and enforcing these Policies.

Qualifications: The Privacy Officer will have experience in information management and be familiar with the day-to-day operations of the Practice, and will have the ability to work well with Practice management, legal counsel, patients, subcontractors, regulatory agencies and law officials. The Privacy Officer will have a strong practical working knowledge of Company operations and of state and federal privacy regulations.

Responsibilities: The Privacy Officer's responsibilities include, but are not limited to, the following:

- developing Company privacy policies and procedures in coordination with Company management and legal counsel
- reviewing, approving and negotiating Business Associate Agreements ("BAAs");
- ensuring BAAs are in place with Company's Business Associates;
- training Workforce members on these Policies;
- responding to patterns of activity or practices that constitute violations of these Policies;
- overseeing prompt and appropriate investigation and resolution of incidents or complaints, including by overseeing investigations of potential Breaches and coordinating applicable notifications required in the event of a Breach;
- implementing steps necessary to mitigate harm caused by violations of the HIPAA Rules or these Policies;
- receiving, processing and implementing requests related to patient rights;
- maintaining documentation required by these Policies;

- making required HIPAA-related reports to patients, the media and HHS and being the point person for interacting with patients and third parties for issues related to compliance with the HIPAA Rules;
- reviewing and revising these Policies as necessary to comply with the HIPAA Rules and changes to Company's operations.

II. Security Officer.

Purpose: The Security Officer is concerned with the overall Protected Data environment and compliance with information security policies.

Qualifications: The Security Officer will have experience in information management and information technology and be familiar with the day-to-day operations of the Practice, and will have the ability to work well with Practice management, legal counsel, patients, subcontractors, regulatory agencies and law officials. The Security Officer will have a strong practical working knowledge of Company operations, in particular the information technology systems and environment used therein, and of state and federal privacy regulations.

Responsibilities: The Security Officer is responsible for overseeing all aspects of information security, including, but not limited to:

- developing and implementing security policies and procedures;
- conducting and facilitating through Human Resources annual Workforce HIPAA security training and issue periodic updates;
- establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations;
- establishing security risk management procedures;
- performing initial and periodic security risk assessments and conducting related ongoing compliance monitoring activities;
- maintaining and implementing policies and procedures to manage Business Associates with whom Protected Data is shared, or that could affect the security of Protected Data;
- maintaining a list of Business Associates;
- maintaining a written agreement BAA that includes an acknowledgement that the Business Associates are responsible for the security of Protected Data the Business Associates receive, store, use or transmit on behalf of Company, or to the extent that they could impact the security of Company Protected Data environment;
- ensuring that there is an established process for engaging Business Associates including proper due diligence prior to engagement;
- maintaining a program to monitor Business Associates' compliance status at least annually;
- ensuring that mechanisms are in place within Company for receiving, documenting, tracking, investigating, and responding to all security related complaints;
- establishing procedures to track access, use and disclosure of Protected Data through information system activity audits, access logs and security incident monitoring; and
- coordinating Breach response procedures with the Privacy Officer.

HIPAA Privacy Policy and Procedure No. 2
Policies, Training and Documentation

Purpose

This policy is designed to ensure the establishment of Company Privacy Policies and Procedures by the Privacy Officer and Security Officer for the purpose of documenting Company obligations as a HIPAA Covered Entity to maintain the privacy of PHI consistent with state and federal privacy laws in accordance with 45 CFR § 164.530, and the requirement that Privacy Officer train its employees regarding such Privacy Policies and Procedures.

Policy

It is Company policy that the Privacy Officer will develop, implement, maintain and update, as needed, Company Privacy Policies and Procedures and will provide training on such policies and procedures, and updates as needed, to Company employees.

All Workforce members must comply with this policy. Violations of this policy may result in disciplinary action, up to and including termination of employment, based on the seriousness of the offense and other relevant factors.

Procedures

Policies and Procedures. Company Privacy Officer, in consultation with its legal counsel, will develop and implement Privacy Policies and Procedures in compliance with the standards and implementation specifications under HIPAA as relate to its provision of healthcare services. The Privacy Officer will amend and update such Policies, in consultation with legal counsel, as necessary to comply with laws and regulations relating to HIPAA Privacy applicable to Company.

Training: Privacy Officer and Human Resources will conduct HIPAA Privacy and Security Training prior to access by a new employee or other Workforce member to PHI.

Training will be provided by the Privacy Officer based on the following schedule:

- New Employees: Within the first three (3) days of hiring and in any event prior to access to PHI;
- Temporary Employees: Within the first three (3) hours of beginning services; and
- Volunteer, Student or similar Workforce: Within the first three (3) hours of beginning services.

The Privacy Officer and Human Resources will maintain the training materials, and any updates, and all certifications of training. Training materials will include, at a minimum, (a) webinar, online or in-person training covering the policies of the Company and HIPAA privacy, security and breach notice requirements; (b) Employee HIPAA Compliance Manual; and (c) periodic privacy and security updates throughout the calendar year.

HIPAA Privacy Policy and Procedure No. 3
Workforce Training

Purpose

The purpose of this document is to establish policies and procedures used by the Company with regard to its employees, contractor and agents ("Workforce") access to the Protected Data environment and the security awareness of those Workforce members.

Policy

A strong Protected Data environment security policy sets the security tone for Company and informs Workforce what is expected of them. It is the policy of the Company to establish security safeguards for permitting Workforce access to its Protected Data and making Workforce aware of the importance of maintaining the security of the Protected Data.

Procedures

1. *Hiring Procedures*. All potential Workforce will be screened prior to hiring to minimize the risk of attacks from internal sources. Background checks include, but are not limited to, previous employment history, criminal record, and reference checks as allowed by relevant laws. Background verification checks on all candidates for employment must be carried out in accordance with relevant laws, regulations and ethics. Background checks should be proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. Human Resources manages this process. In the event of an incident or for other good cause, additional background checks may be performed during employment. The Company will conduct background checks in compliance with the federal Fair Credit Reporting Act (FCRA), the Americans with Disabilities Act (ADA), and all other applicable local, state, and federal laws and regulations. Applicants and employees may request and receive a copy of requested "investigative consumer reports."

2. *Security Awareness Training*. A formal Security awareness program shall be implemented and provided by Human Resources to make all Workforce aware of the importance of Protected Data security. All Workforce that access Protected Data must receive appropriate awareness training and regular updates, as applicable for their job function upon hire and at least annually. All Workforce will be required to participate in security awareness training at least annually. Periodic security awareness reminders or updates will be provided as needed. Human Resources shall maintain a copy of all training materials, updates and verification of training completion. Failure to complete annual security training is a basis for disciplinary action.

3. *Initial Security Orientation*. New Workforce must be made aware of and receive training on Company policies and procedures as a part of their orientation prior to access to Protected Data. Documentation of training and updates and specific attendance and

completion shall be maintained in Workforce employment file by Human Resources and by the Security Officer.

4. *Off-boarding Procedures*. Company will utilize an off-boarding checklist that addresses the following items:

    a. When a Workforce employment, arrangement or contract is terminated, Human Resources will then initiate the formal procedure for offboarding including notifications for removal of access to all electronic systems and the building. Human Resources should coordinate with the Workforce supervisor to secure the workspace at the time of termination and prevent access to it after termination. Arrangements should be made to collect all personal belongings and deliver to the employee. Human Resources should notify: the IT manager, any Business Associate who has granted the Workforce access to Protected Data, Workforce manager, and building manager, each to the extent applicable.

    b. The Information Technology Manager will:
        i. revoke all user IDs associated with the individual immediately;
        ii. terminate access to Company email and freeze and archive the individual's email account;
        iii. reset all relevant passwords (wireless, system access);
        iv. perform an audit log if off-boarding was involuntary and suspected violation of privacy and/or security policies occurred and a log of all accesses and activity with the individual's credentials during the time in question shall be maintained by the Security Officer;
        v. prior to repurposing returned equipment, IT manager must follow the policies set out in the Data Destruction Policy and will make a copy of the hard-drive for storage, if any suspected violations of data privacy and security policies, laws or regulations is suspected. The hard-drive copy shall be maintained securely by the Security Officer. Forensic exam of equipment may be required prior to destruction and repurposing.

    c. The Workforce's supervisor, in coordination with Human Resources, is responsible for (each to the extent applicable):
        i. ensuring return of all property in the custody of the individual, including all computer equipment, is returned to Company;
        ii. all system or facility access cards, facility keys, and identification badges are retrieved from the individual prior to the departure; and
        iii. ensuring that access cards are immediately deactivated.

5. *Disciplinary Procedures*. Workforce security training will include a description of the disciplinary penalties for violation of the Security policies and procedures. Each employee must acknowledge these procedures as detailed in the security policies and in the employee handbook prior to access to Protected Data. Depending on the conduct, disciplinary steps may include without limitation: oral warnings, written warnings, use of a performance improvement plan, or termination. Factors that may be considered in ascertaining the appropriate steps may include without limitation: seriousness of conduct; employment record; individual's ability to correct conduct; action taken with respect to

similar conduct by other individuals; effect on members or other external relationships such as vendors and job candidates; surrounding circumstances; and other job-related factors.

HIPAA Privacy Policy and Procedure No. 4
Workforce Reporting Violations, Sanctions and Mitigation

Purpose

To describe the reporting process associated with violations of privacy policies and procedures, the circumstances under which sanctions may be imposed against a Workforce member who violates Company privacy policies and procedures, and to describe measures that may be needed to mitigate possible harm caused by such violations in keeping with Company obligations to maintain the privacy of PHI consistent with state and federal privacy laws in accordance with 45 CFR §§ 160.316, 164.530 (e), (f) and (g), and 164.502(j).

Policy

It is Company policy that violations of privacy policies and procedures are identified and addressed promptly, that appropriate sanctions are implemented, and that appropriate measures are taken to mitigate any impermissible access, use, disclosure, modification or destruction of PHI in order to reduce the possibility of harm.

All Workforce members must comply with this policy. Violations of this policy will result in disciplinary action based on the seriousness of the offense or other factors. Disciplinary action may include written warning, suspension, or termination.

Procedures

1. *Process of Reporting*.

   a. All Company Workforce members will report violations of Company privacy policies and procedures (including self-reporting) to their supervisor and the Privacy Officer.

   b. Company will investigate the reported violation and document the findings.

   b. The Privacy Officer will document and account for any impermissible disclosure in the Accounting for Disclosures Log.

2. *Sanctions*. The Human Resources Department, in consultation with Privacy Officer, will establish a range of sanctions that may be imposed if Company privacy policies and procedures are violated, as may be more particularly set forth in a separate *HIPAA Privacy Policy and Procedure - Santions*. Disciplinary action will be commensurate with the severity of the violation, the intent, the existence of previous violations and the degree of potential harm. Sanctions may range from warnings and further training, in the event the Workforce member was not aware of policy requirements, to termination of employment in the event of a knowing and intentional violation. All Company Workforce members will be made aware of the disciplinary actions and sanctions that may be imposed. Additionally, federal privacy laws impose civil and criminal penalties, including possible fines and imprisonment for violations of the law.

3. *Mitigation*.

   a. Upon discovering that Company privacy policies may have been violated, the Privacy Officer will investigate the possible violation and take any appropriate mitigating measures to the extent practicable.

b. If the terms of a Business Associate Agreement ("BAA") have been violated, the Privacy Officer will consult the BAA, give notice to the applicable Business Associate and follow the requirements for cure and/or termination outlined in the BAA. If the Business Associate persists in the violation, the BAA and any associated service agreement must be terminated.

4. *No Sanctions or Retaliation Based on Whistleblowing or Objections*.

a. It is not a violation of Company privacy policies for Company Workforce member to disclose Individually Identifiable Information to a health oversight agency, public health authority, attorney or other appropriate entity in the good faith belief that Company or a Company member has engaged in unlawful conduct, violated professional or clinical standards, or potentially endangered Patients, workers, or the public. Sanctions will not be imposed based on such good faith actions.

b. It is not a violation of Company privacy policies for Company Workforce member who is the victim of a criminal act to disclose information about the suspected perpetrator to a law enforcement agency, as long as the officer or agency's identity and authority has been verified and documented and the disclosure is limited to the "minimum necessary" information needed to carry out the purpose. Sanctions will not be imposed based on such actions.

c. It is not a violation of Company privacy policies for Company Workforce member to file a complaint with the Secretary of HHS, testify, assist, or participate in an investigation or compliance review of Company privacy policies, or oppose any act made unlawful by the federal privacy regulations, provided the Workforce member has a good faith belief that Company action being opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of PHI in violation of the federal privacy regulations. Sanctions will not be imposed based on such actions.

5. HIPAA Fines and Penalties. A violation of HIPAA Privacy and/or Security Policies may result in civil and/or criminal liability for Company and/or for the Workforce member(s) participating in the violation. A failure to report a known breach by another person or a business associate may itself be a violation of HIPAA. The Secretary of the Department of Health and Human Services (HHS) has discretion in determining the amount of the penalty based on the nature and extent of the violation and the nature and extent of the harm resulting from the violation.

The Secretary will not impose civil penalties (except in cases of willful neglect) if the violation is corrected within thirty (30) days. Therefore, prompt reporting and responsive corrective action are imperative. For that reason, among others, self-reporting is encouraged. Company has a non-retaliation policy.

HIPAA Privacy Policy and Procedure No. 5
Minimum Necessary and Uses and Disclosures

Purpose

To describe and establish procedures for determining the extent to which Company, its employees and agents, may use or disclose PHI on behalf of Company.

Policy

It is Company policy to limit use or disclosure of PHI by its employees, agents and business associates as required by HIPAA and in accordance with the Minimum Necessary standard under HIPAA.

Procedures

1. To protect the privacy of patients, most requests, uses or disclosures of patient information should be limited to the minimum amount of information reasonably needed to accomplish the purpose for which the information is being used or disclosed. This means that reasonable efforts should be made not to use or disclose information that is not relevant or that exceeds the amount requested. Company may not require an Patient to waive their rights related to PHI as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

2. The "minimum necessary" limitations do not apply to information being requested by or disclosed to any of the following:

- Patient or authorized Patient Representative
- Healthcare provider for Treatment
- Person or organization named in a valid authorization
- Secretary of Health and Human Services
- Official or agency required by law
- Uses or disclosures required to comply with HIPAA.

3. A role-based protocol will be used. Company should identify those staff members (*e.g.*, medical assistants) who need access to health information to carry out their duties, the category or categories of health information to which such staff members need access, and any limitations or conditions appropriate to such access. Staff members of Company generally should only be allowed access to those portions of the Patient's medical record reasonably needed in order to perform their job functions. To the extent reasonably possible, access to electronic health information should be limited through role-based access controls that allow only authorized individuals to obtain access to various levels of information.

4. "Routine" disclosures are disclosures that are made on a recurring basis. Company should identify those persons and entities to whom routine disclosures are made, and determine the categories of health information reasonably needed for them to carry out the purpose for which the disclosure is made.

5. For non-routine requests and disclosures (*i.e.*, those that are not made on a recurring basis and for which Company has not established policies and procedures), medical records must be reviewed on a case-by-case basis by the Privacy Officer to determine the minimum necessary amount of information that may be disclosed. For subpoena requests for records, the minimum necessary is deemed to be the amount sought by the subpoena, as determined by the Privacy Officer.

6. Unless otherwise indicated by the circumstances, Company may rely on the requestor's statement that the information requested for any of the following purposes has been limited to the minimum necessary for the stated purpose:

- Disclosures requested by public officials for public health purposes, health oversight, law enforcement, or other permitted disclosures, if the official represents that the information requested is the minimum necessary for the stated purpose;
- Disclosures requested by other health care providers or covered entities, such as treatment providers and health plans;
- Disclosures requested by a professional who is either (i) a member of Company or (ii) a business associate providing professional services and who has executed a valid business associate agreement that includes representations that he or she will only request the minimum necessary information required for the professional to provide such services; and
- Disclosures for certain research purposes to a person or entity that provides appropriate documentation in accordance with Section 164.512(i) of the privacy regulations.

7. When Company requests patient health information from other entities, Company shall request only the minimum amount of information to carry out the purposes for which the information is requested. Non-routine requests must be approved by the Privacy Officer to ensure that only the minimum necessary information is requested.

8. Company must require its business associates to comply with HIPAA's minimum necessary rule as well as Company minimum necessary policies and procedures, to the degree applicable.

9. In general, PHI used internally at Company may be used by Company personnel for treatment purposes. Only the minimum necessary PHI shall be disclosed for payment functions.

10. The minimum necessary does not apply to disclosures ordered from an administrative tribunal or by order of court; however, only the specific information identified in the order should be disclosed. The minimum necessary standard shall apply to information released to a law enforcement regarding victims of crime or abuse. However, if the law requires information to be released, then the disclosure will be in compliance with the subpoena, statute, or law.

11. PHI may be disclosed to comply with workers' compensation laws and regulations without consent, authorization, or opportunity to object by the Patient, but such disclosure shall be the minimum necessary.

12. Unless specifically justified as being the minimum amount necessary for the purpose, the complete medical record should not be requested or disclosed.

13. An incidental Use or Disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and occurs as a by-product or an otherwise permitted use or disclosure. Examples of incidental uses or disclosures include: (1) use of a patient sign-in sheet or announcing a patient's name in the waiting room, (2) discussions in a joint treatment room, as long as the tone of discussion remains low, and if the Patient has no objection, or (3) identification of a Patient on a treatment room door or paper file. Company has assessed risk areas to implement safeguards intended to limit incidental uses or disclosures and has implemented safeguards accordingly.

14. Sensitive information is information that is more likely to result in harm, embarrassment, or unfairness to an Patient. Examples of sensitive information may include information related to HIV/AIDS information, substance abuse treatment information, and mental health information. Additional precautions should be taken with sensitive information. To the extent that Company receives a request to disclose or otherwise use sensitive information, including psychotherapy notes, such request should be relayed to Privacy Officer, as appropriate to ensure such use and disclosure is proper/secure.

15. Please contact the Privacy Officer should you have any questions concerning the application of the minimum necessary standard to any particular, use, disclosure or request for PHI.

HIPAA Privacy Policy and Procedure No. 6
Safeguards

Purpose

This Policy and Procedure details the information safeguards required of all Workforce members in order to ensure adherence to privacy requirements consistent with Company obligation to maintain the privacy of PHI pursuant to state and federal privacy laws.

Policy

Company will maintain appropriate administrative, technical and physical safeguards to protect the confidentiality, integrity and accessibility of PHI consistent with the requirements of these HIPAA Privacy Policies and to safeguard PHI from intentional and unintentional non-permissible uses and disclosures. These safeguards will supplement and be consistent with security measures and policies followed by Company with respect to the IT environment.

General Safeguards

Safeguards employed by Company will include the following:

(a) Restricting access to files containing PHI to only Workforce members.

(b) Storing files containing PHI in a secure location when not in use (i.e., locked room or file cabinet). Under no circumstances should PHI ever be saved or written to unencrypted flash drives. If you intend to use flash drives or other portable devices to store or transmit PHI, such device must be encrypted and tracked by the IT department.

(c) Using reasonable safeguards so that PHI on computer screens will not be visible to unauthorized persons, including locking down computer workstations when not in use or when leaving the workstation by activating a password protected screen saver and clearing PHI from the computer screen when the PHI is not actually being used.

(d) Ensuring firewalls are in place to protect ePHI.

(e) Prior to discarding PHI, securely destroying PHI by, among other things, shredding documents or destroying hardware that contain PHI so that they cannot be read or reconstructed.

(f) Not holding phone conversations or other discussions in areas where unauthorized persons may overhear. Phone conversations involving PHI should not be held on speakerphone, unless everyone within listening distance is an authorized recipient of the PHI.

(g) Marking documents containing PHI that are delivered by mail or hand delivery as "confidential."

Paper and Fax Safeguards

Company will take reasonable steps to send and receive facsimile transmissions securely, including the following safeguards:

(a) Printers and fax machines should not be located in areas with public access.

(b) Faxes: When faxing PHI, Workforce members will use a Company cover sheet (with standard confidentiality disclaimer) and will verify the accuracy of the fax number before transmitting. No PHI will appear on the cover sheet.

(c) Paper copies of documents containing PHI should be printed only if necessary in order to complete the Workforce member's job duties. Paper copies should never be printed merely for convenience. Upon completion of the duty, if the paper copy is not required to be maintained, it must be immediately shredded. If the paper copy must be maintained, it must filed in the appropriate location immediately.

(d) Printed documents containing PHI should never be left on the printer. As soon as the Workforce member hits the "print" button, he or she should retrieve the document from the printer.

(e) Excess or unneeded copies of printed documents containing PHI must be shredded or placed in secured shred collection containers that are serviced by corporate-approved vendors. Workforce members should never place un-shredded documents containing PHI into a trash receptacle.

(f) Company maintains a "clean desk" policy. Paper documents containing PHI should never be left out on an Workforce member's desk when the Workforce member is away from his or her desk. At any temporary absences during the workday, the Workforce member must place the documents into a desk drawer if available, and must, at a minimum, place such documents face down on the desk.

(g) At the end of the workday, any and all documents containing PHI must be placed in a locked cabinet within a locked room. Under no circumstances should any documents containing PHI be left on a desk or otherwise unsecured overnight.

E-mail and Network Safeguards

Strong encryption must be used to safeguard Protected Data during transmission over email, open, public networks including the Internet, wireless technologies, cellular technologies, and other electronic communication methods. The most current secure protocols recommended by NIST must be utilized to safeguard Protected Data.

Computers

Only those Workforce members with a legitimate business need for a laptop will be issued a laptop computer. The preference instead will always be for the use of a desktop computer. Laptops may be issued only with the advance written approval of an authorized representative of the Privacy Officer.

(a) Computer monitors should be positioned on Workforce members' desks in a manner that does not allow the screen to be seen by persons who do not have a need to see the data.

(b) When leaving their workstations unattended, Workforce members will lock their computer screens by enabling a password protected screen saver or timeout process or by shutting their computer down.

(c) All laptops must configured and password protected as specified by the HIPAA Security Policies. Under no circumstances should an Workforce member share or allow any other individual to use their password.

(d) Any equipment storing PHI should be encrypted.

(e) Workforce members may not allow access to Company's secure network by unauthorized persons.Mobile Devises

Mobile Devices

(a) Company e-mail accounts should be accessed using a smart phone, tablet or similar device only if necessary in order for an Workforce member to complete his or her duties.

(b) Use of smart phones, tablets or similar devices must comply with the Company's Security Policies regarding mobile devices.

(c) Workforce members should never include PHI in an unencrypted text or email message.

(d) Bluetooth should be disabled when device is in a public location or could be synced to a presentation screen.

Transportation of PHI

PHI, regardless of format or medium, should only leave the property of Company if required in order for the Workforce member to complete his or her job duties. The presumption is always that PHI never leaves the property of Company, and each Workforce member has the responsibility and burden of ensuring that PHI only leaves the property of Company when absolutely required in order to complete the Workforce member's job duties. Workforce members are responsible for securing PHI in their possession during transit.

Working at Home

Any Workforce member working at home or at other teleworking environments will ensure the following:

(a) Visitors and family members do not have access to Company documents, computers or media containing PHI.

(b) PHI in any format is not visible to unauthorized viewers.

(c) Company owned laptops and mobile devices are secured at all times and not left in vehicles or public locations, including hotel concierge services.

(d) Electronic PHI is never stored on non-Company owned computers and is only stored on Company secure computer system environment.

HIPAA Privacy Policy and Procedure No. 7
Accounting of Disclosures

Purpose

To describe the circumstances under which a Patient or Patient Representative may obtain an accounting of certain disclosures of their PHI and how Company will respond to requests for accountings consistent with state and federal privacy laws and in accordance with 45 CFR § 164.528.

Policy

It is the policy of Company to provide Patients or Patient Personal Representatives with an accounting of any PHI disclosures that are requested by the Patient or Patient Personal Representative.

All Workforce members must comply with this policy. Violations of this policy will result in disciplinary action, up to and including termination of employment, based on the seriousness of the offense or other factors.

Procedures

1. *Right to Accounting of Disclosures*. Patients have the right to receive an accounting of certain disclosures of their PHI made by Company. Only the Patient or the Patient's Personal Representative may obtain an accounting of the disclosures of a Patient's PHI.

   a. Except as provided in Paragraph 1(c) below, the accounting must include all disclosures made for purposes other than those identified below within the six (6) years prior to the date on which the accounting is requested. The accounting does NOT include disclosures made for the following purposes or to the following recipients:

      i. For treatment, payment, or healthcare operations;

      ii. To the Patient or the Patient's Personal Representative;

      iii. Authorized by the Patient or the Patient's Personal Representative;

      iv. To notify families of Patients or to assist families or and other persons involved in the Patient's care;

      v. For national security intelligence;

      vi. To correctional institutions or to law enforcement authorities that have custody of the Patient;

      vii. Consisting only of de-identified information;

      viii. Incident to a use or disclosure otherwise permitted or required by these policies; or

      ix. As a part of a limited data set in accordance with §164.514(e).

   b. Examples of accountable disclosures include:

      i. Non-permitted disclosures known to any Company Workforce members;

      ii. Disclosures to government agencies performing licensure surveys and other healthcare oversight activities;

iii. Disclosures made pursuant to a court order or subpoena;

iv. Disclosures to law enforcement; and

v. Disclosures about victims of abuse, neglect or domestic violence.

c. If law enforcement requests delay of disclosure in writing, Company must delay disclosure of accounting. Any such delay must be added to the *Accounting of Disclosure Log*.

2. *Accounting of Disclosures Log*. If a log is not created or maintained in the electronic health record, then a form may be created to account for disclosures with a copy maintained in the applicable Patient record and by the Privacy Officer.

3. *Requests Made by Patients or Personal Representatives of Patients*.

a. Upon receiving a request for an accounting of certain disclosures of their PHI directly from a Patient or a Patient's Personal Representative, Company Workforce member will refer the Patient or Patient's Personal Representative to the Privacy Officer, which will oversee the response.

b. No later than sixty (60) days after Company receives the request for an accounting, the Privacy Officer will either:

i. Provide the Patient with the requested accounting; or

ii. If the Privacy Officer is unable to provide the accounting within sixty (60) days, provide the Patient with a written statement explaining the reason(s) for the delay and the date by which the accounting will be provided, which shall be no more than thirty (30) days following the expiration of the initial 60-day deadline.

4. *Requests Made via a Business Associate*.

a. Upon receiving a request for an accounting of certain disclosures of PHI from a Patient, the Business Associate Workforce member is required under our BAA to forward the request to Company Privacy Officer, which will oversee the response. Company Privacy Officer will contact the Business Associate Privacy Officer in a manner that complies with the applicable BAA. Company Privacy Officer is responsible for making determinations regarding requests for accountings.

b. Business Associate's Privacy Officer will provide to Company an Accounting of Disclosures within thirty (30) days of Company or the Business Associate's receipt of an authorized request, unless the BAA requires a quicker response.

5. *Charges*.

a. Company shall not charge for the first accounting but may charge a reasonable, cost-based fee for any additional accounting requests received within a twelve (12) month period following the first request, provided the Patient or Patient's Personal Representative is informed in advance of the fee and is provided with an opportunity to withdraw or modify the request for a subsequent accounting.

b. For disclosures of PHI maintained in an electronic health record, the charge for disclosure may not exceed labor costs.

c. Company Privacy Officer will determine if a charge for disclosure is appropriate.

6. *Provision of Accounting*.

a. Accountings of Disclosures provided by Company Privacy Officer will include the following information:

   i. The date of the disclosure;

   ii. A brief description of the types of PHI disclosed;

   iii. Name of entity or person who received the PHI and address if known; and

   iv. A brief statement of the purpose of the disclosure that reasonably informs the Patient of the basis for the disclosure or, in lieu (or in addition to) of such statement, a copy of a written request for disclosure, if any.

b. If multiple disclosures are made to the same person or entity for a single purpose, a single accounting may be provided that includes the above information, and period during which disclosures were made and the last date of disclosure.

c. Research disclosures for 50 or more patients: If it is likely that an individual's PHI was disclosed, then Company shall assist Patient, if requested, in contacting the sponsor and/or researcher to whom the PHI was disclosed. The accounting should include:

   i. name of the protocol or research activity;

   ii. description of research, purpose and criteria for selecting records;

   iii. brief description of PHI disclosed;

   iv. period of time during which disclosures were made;

   v. name, address and phone number for the research sponsor and the researcher to whom the PHI was disclosed;

   vi. the following statement, "Your PHI may or may not have been disclosed for *[Protocol]* or other research activity."

7. *Accounting for Disclosures*: Logs of PHI disclosures required for an Accounting for Disclosure to a Patient for disclosures outside of treatment, payment and healthcare operations and to Business Associates must be maintained for a minimum of six (6) years.

HIPAA Privacy Policy and Procedure No. 8
Amendment of PHI

Purpose

To describe the circumstances under which an Patient or Patient's Representative is entitled to request amendment of PHI and how Company will respond to any request for such request for amendment consistent with state and federal privacy laws and in accordance with 45 CFR § 164.526.

Policy

It is Company policy to allow amendments to be made to an Patient's PHI in accordance with state and federal laws.

All Workforce members must comply with this policy. Violations of this policy will result in disciplinary action, up to and including termination of employment, based on the seriousness of the offense or other factors.

Procedures

1. *Patient's Right to Amend*. All Patients or Patient Representatives have the right to request amendment of their health records. Only the Patient or the Patient's Representative may request an amendment.

2. *Responsibility for Amendment Determinations*.

    a. Privacy Officer is responsible for granting or denying amendment requests made to Company.
    b. Any Workforce member that receives a notice from a Patient or Patient's Personal Representative that Company either amend an Patient's health record or assist in evaluating an amendment request will forward the notice to Privacy Officer which will oversee responding to and handling the notice.

3. *Requests from Patients or Personal Representatives*.

    a. Any request by a Patient or Personal Representative of a Patient to amend such Patient's health record must be made in writing and submitted to the Privacy Officer. Any such request must be supported by a stated reason(s) for the requested amendment.
    b. The Privacy Officer will consider any such submitted request and will make a determination of whether to grant the request within sixty (60) days. If such a request cannot be acted on within sixty (60) days, the Privacy Officer may take an additional thirty (30) days to act upon the request, provided the Privacy Officer provides appropriate notice and explanation to the requesting Patient. Written notice to the Patient must be delivered within sixty (60) days advising whether the request is approved or denied, and if additional time for action is required.

c. If the request is granted, the Privacy Officer will oversee and direct the making of the amendment, as well as ensuring the requesting Patient and other relevant persons are notified, as appropriate.
d. If the request is denied, the Privacy Officer must provide the requesting Patient with a written denial, detailing the basis for the denial and the Patient's right to submit a written statement of disagreement and/or file a complaint regarding the denial.

4. *Requests from Company Patients or Personal Representatives of Patients made via a Business Associate*. If a Company Workforce member is informed by a Business Associate of a request to amend a Patient's health record, he or she must notify Company Privacy Officer.

5. *Acceptance of Amendment*. If the request is accepted, the amendment must be included in the Patient's record. It may either be attached to the original entry or a notation may be written in the margin of the original entry showing where the amendment is located in the record. If the amendment affects several parts of the record, all such parts should be appropriately marked to show the correction. Amendments to an electronic health record will be made in accordance with applicable protocols that preserve the original version.

Never delete or erase the original information in the Patient's medical record, even if it is found to be incorrect. However, if necessary in order to avoid confusion or harmful reliance on incorrect information, a medical professional may draw a single line through the incorrect information and initial and date the modification, as long as this is in keeping with accepted professional practices.

6. *Notifying Others of Amendment*. The amended information should be sent to anyone to whom Company may have sent the original incorrect or incomplete information, if such persons might possibly harm the Patient by relying on incorrect or incomplete information. The Patient should be asked to supply names and addresses of anyone the Patient believes needs to be notified. Company must notify its business associates to amend their records as well.

7. *Basis for Denial*. The request may be denied, in whole or in part, for any of the following reasons:

- The information is not part of the Patient's medical records, payment and insurance records, or any other collection of health information maintained and used by Company to make decisions about the Patient.
- The information was not created by Company, and therefore the Patient should go to the original source of the information to seek an amendment.
- The information in Company record is already reasonably accurate and complete, and the proposed amendment does not provide further clarification or new information needed in order to properly treat the Patient.

8. *Procedure for Denial*. If Workforce Member denies the requested amendment, Workforce Member provides a written denial to the Patient which contains:

- Basis for denial;
- A statement that the Patient has the right to submit a written statement disagreeing with the denial and how the Patient may file such a statement;

- A statement that if the Patient does not submit a statement of disagreement, the Patient may request that Company provide the Patient's request for amendment and the denial with future disclosures of related PHI; and
- A description of how the Patient may file a complaint with Company or the Secretary.

Company may prepare a written rebuttal to the Patient's statement of disagreement and must provide a copy to the Patient.

HIPAA Privacy Policy and Procedure No. 9
Patient Requests for PHI

Purpose

To describe the circumstances under which a Patient is entitled to inspect and obtain copies of their health record maintained by Company and how Company will respond to requests for access, consistent with state and federal privacy laws and in accordance with 45 CFR § 164.524.

Policy

It is Company policy to allow Patients or Patients' Personal Representatives to inspect and obtain copies of their PHI in accordance with state and federal laws.
All Workforce members must comply with this policy. Violations of this policy will result in disciplinary action, up to and including termination of employment, based on the seriousness of the offense or other factors.

Procedures

1. Right to Inspect Health Record. Patients or Patients' Personal Representatives generally have the right to inspect and obtain copies of their health information.

Company may request that the request be submitted in writing, provided Company has previously informed the Patients of this requirement, using a specified form and may also permit requests electronically by email or patient portal through a specified form. However, Company may not require use of a web portal if a Company does not have internet access. See Form ***Request for Copy of Records***. Company may not require that a Patient return this form by mail to receive a copy of the records.

Records to be provided do NOT include those set forth in Section 3 of this Policy hereinbelow.

2. Providing Access and/or a copy of the Records.

(a) The Privacy Officer is responsible for granting or denying access requests made directly to Company.
(b) Any Workforce member who receives a request for health records will forward the request immediately to Privacy Officer, who will oversee the response.
(c) Any request by a Patient or Personal Representative of a Patient to inspect and/or obtain a copy of the Patient's health information maintained by Company should be made in writing and submitted to the Privacy Officer. See Form ***Request for Copy of Records***.
(d) The Privacy Officer will consider any such submitted request and will make a determination of whether to grant the request within thirty (30) days. If such a request cannot be acted on within thirty (30) days, the Privacy Officer may take an additional thirty (30) days to act upon the request, provided the Privacy Officer provides appropriate written notice and explanation to the requesting Patient.

(e) Company must use its authentication processes to verify the Records belong to the Patient. Company must not disclose information without verification.
(f) If the request is granted, the Privacy Officer will oversee and direct the provision of access and/or copies by the Medical Records Department.
(g) If the request is denied, the Privacy Officer will provide the requesting Patient with a written denial within thirty (30) days, detailing the basis for the denial and the Patient's review rights (if applicable), as well as the Patient's right to file a complaint with Company or the HHS Secretary regarding the denial.
(h) If a Patient has questions regarding the Records, Company is not required to interpret any part of the Record, diagnosis or test results, and should refer the Patient to the treating provider for a consultation.
(i) If the PHI is maintained by a Business Associate, Company must promptly notify the Business Associate that access should be provided and the time frame required for response. The applicable Business Associate Agreement should be checked to verify time frame and contact information.

3. Denial of Request. Under certain limited circumstances, Company may deny a Patient's request for records access. Certain of these denials are not reviewable.

Unreviewable denials:

- Requests for psychotherapy notes
- Requests for information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding
- Requests by an inmate for PHI held by a correctional institution
- Requests for PHI in an ongoing research study conditioned on individual's agreement to suspend access in the consent to participate (access reinstated at completion of study)
- Requests PHI in Privacy Act protected records such as records under control of a federal agency
- Requests for PHI obtained by someone other than Company under a confidentiality agreement and disclosure would reveal the identity of the source

Reviewable denials:

- Access is reasonably likely to endanger the life or physical safety of the individual or another person not including concerns about psychological or emotional harm
- Access is reasonably likely to cause substantial harm to a person, other than Company, referenced in the PHI
- Access to the personal representative requesting the PHI is reasonably likely to cause substantial harm to the individual or another person

Company may not require that a Patient or personal representative provide reason or rationale for requesting the records and Company may not deny access based on the reason or rationale.

4. Fees for Records. Company may charge the Patient a reasonable fee for the cost of preparation and transmittal of the requested Patient records that exist in a physical format; this includes the labor, supplies and postage and cost of preparing a summary if Patient agrees to a Summary. Notwithstanding the foreging, Company may ***not*** charge a Patient for access to the

PHI in Patient's electronic health record. Company may (1) calculate the actual allowable costs to fulfill each request; or (2) use a schedule of costs based on average allowable labor costs to fulfill standard requests; or (3) if the records are maintained electronically, Company may charge a flat fee of $6.50 per request. The flat fee is not a maximum fee that may be charged for electronic records. The applicable fee may not exceed any applicable state law fee limits.

Costs include only the labor for creating and delivering the copy of the PHI but not time for reviewing the request, and for search and retrieval of the records. Cost may be calculated based on the actual time required to make and send the record in the form and format requested times the reasonable hourly rate of the person making the copy. The hourly rate may vary depending on whether the record is in paper (administrative labor) or electronic (technical skilled labor to convert and transmit PHI in a particular format), and the cost of the material or portable media.

NOTE: Company may not withhold production of records on the grounds that Patient has an outstanding balance.

5. Form and Format of Records. Company must provide the records in the form and format requested by the Patient if the record is readily producible in that form. If records are maintained electronically, then records must be produced in an electronic format requested. If not readily available, then a machine readable copy (such as a pdf) is sufficient. Company may provide the Patient with a summary or explanation of the PHI requested, in lieu of providing access to the record, if the Patient agrees in advance to the summary and to the fees imposed, if any, for the summary or explanation.

6. Delivery. If the Patient requests that a copy of the record be sent directly to another person, Company must comply with the request, provided the request is in writing, signed by the Patient, and clearly identifies the designated person and where to send the copy of the information. An Authorization is not required if the Patient requests the copy. If delivery is to the Patient, then the delivery method specified by the Patient should be followed if feasible. If no method was specified, the delivery by mail to the Patient's home address is acceptable unless the Patient has restricted communications at home. The fee restriction applicable to records delivered to the Patient does not apply to records delivered to a third-party at the Patient's direction.

7. Encryption. If the Patient requests an electronic copy of the health record, then such information should be delivered in encrypted format with a decryption password delivered in a separate communication. If delivered by encrypted email, then the password should be delivered by a separate email. If delivered by flash-drive, DVD or other portable storage device, then the device must be encrypted and delivered with tracking and the password must be delivered separately by either email or tracked mailing service. If the health record is delivered through an electronic file-sharing service, Company must verify that such service is secure in accordance with HIPAA security requirements, and has the ability to provide access to Company if requested. Any file-sharing service must be subject to a Business Associate Agreement with Company. If the Patient requests an unencrypted electronic copy, then the Patient should be made aware of the risks of transmission or delivery of an unencrypted electronic health and execute a release and waiver acknowledging risks.

8. Request for Deceased Patient Records.

A. If a request is received for a copy of a deceased Patient records, and it is determined that the requestor is the deceased Patient's legal representative, then a full copy of the record may be provided to the same extent it would have been provided to the Patient while living. If the requestor is a family member, caretaker or other person involved in the Patient's care or payment for care, then that part of the medical record related to the requestor's involvement may be provided. In each instance, the request should be made in writing. See Form ***Request for Copy of Records of Deceased Patient.***

B. Company may disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased Patient, determining a cause of death, or performing other duties authorized by law. Company may disclose PHI to a funeral director, as provided by law, as is necessary for the funeral director to carry out his or her duties with respect to the decedent. If disclosure of PHI is necessary for the funeral director to carry out his or her duties, Company may disclose the PHI prior to, and in reasonable anticipation of, the Patient's death.

HIPAA Privacy Policy and Procedure No. 10
Notice of Privacy Practices

Purpose

To describe the content and publication requirements for a Notice of Privacy Practices to be used by Company as required by 45 CFR §164.520 and the language requirements under Section 1557 of the Affordable Care Act (ACA), and to establish the process for receiving and responding to Patient complaints or concerns related to Company Notice of Privacy Practices.

Policy

It is the policy of Company to disclose its Notice of Privacy Practices to each new Patient, provide a copy of such Notice upon request, and to prominently display the Notice at each location and on the Company website. Patients have the right, free of the fear of retaliation, to make a complaint or grievance expressing concerns related to the Company's Notice of Privacy Practices.

Procedures

1. *Notice of Privacy Practices*: The Notice shall describe in plain language and with sufficient detail the following:

With regard to uses and disclosures:

a. In a header: "**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**."
b. The permitted uses and disclosures of PHI which Company may make for treatment, payment and healthcare operations with at least one example each;
c. Other purposes for which Company is permitted or may be required to disclose PHI without a Patient's authorization;
d. Any HIPAA permitted or required disclosure which is prohibited or restricted by more stringent state or federal law;
e. The types of uses and disclosures that require authorization; notice that such uses and disclosures will not be made without authorization and notice that authorization may be revoked at any time;
f. Company may contact the Patient to provide appointment reminders or information about treatment options or other health related benefits and services that may be of interest to the Patient; and
g. Company may contact the Patient with fundraising information and the Patient may opt-out of receiving such communications.

With regard to the Patient's rights:

a. the right to notification in the event of a breach;

b. the right to request restriction of certain uses and disclosure but Company is not required to agree to the restriction except for a restriction of disclosures to a health plan when the Patient has paid for the services out of pocket and in full;
c. the right to confidential communications of PHI;
d. the right to inspect and receive a copy of PHI, either in paper or electronic form;
e. the right to amend the Patient's PHI;
f. the right to receive an accounting of disclosures of PHI, except for disclosures made for treatment, payment or healthcare operations, to a business associate, and other limited circumstances; and
g. the right to receive a paper copy of the Notice of Privacy Companys.

With regard to Company obligations:

a. Company is required by law to maintain the privacy of PHI, to notify Patients of its legal duties and privacy practices and following a breach of unsecure PHI;
b. Company is required to abide by the terms of the current Notice but reserves the right to change a privacy Company prior to issuance of a revised Notice;
c. Company may change the terms of the Notice and make the revised Notice applicable to PHI it maintains; and
d. A description of how a revised Notice will be made available to Patients (i.e., posted in the office, posted on the website).

Complaints:

a. If a Patient feels that there has been a violation of the Patient's privacy rights, the Patient may file a complaint with Company and with the Secretary of Health and Human Services;
b. A description of how to submit a complaint to Company; and
c. A statement that Company will not retaliate against the Patient for submission of a complaint.

Contact information and effective date:

a. Name, title and phone number of person to contact for more information (typically the Privacy Officer); and
b. Effective date of the Notice.

Revisions: Company must revise its Notice when there has been a material change in:

a. Uses and disclosures of PHI by Company;
b. Patient's rights (as in an amendment of HIPAA or other law affecting uses and disclosures);
c. Company legal duties (as in an amendment of HIPAA or other law affecting uses and disclosures); or
d. Other privacy practices identified in the Notice.

Company may not implement any such material change prior to revision of its Notice, except when required by law.

Non-discrimination: Pursuant to non-discrimination provisions of Section 1557 of the ACA, the Notice will include a Notice of Non-discrimination and appropriate language assistance taglines consistent with HHS guidance.

Other procedures:

a. Company must provide the Notice to a new Patient no later than the date of service delivery. Company should obtain an acknowledgment of receipt of the Notice or, if acknowledgement could not be obtained, documentation of good faith effort to obtain acknowledgement;
b. Company must post the Notice in a clear and prominent location for a Patient to read (posting in the registration area and having a laminated copy for reading is sufficient);
c. Company must post the Notice prominently on its website;
d. Company must include its notice of non-discrimination and language assistance taglines in the 15 languages identified by HHS for Company location or such other 15 languages that Company determines are needed to satisfy the Section 1557 language nondiscrimination requirements;
e. Company may deliver the Notice electronically by email if the Patient has consented to communication by email but must still maintain a hard copy for delivery to the Patient if requested;
f. Company must have a copy of the Notice available for a Patient to take if it is requested or if electronic delivery failed;
g. Joint Notice may be provided for covered entities in an organized healthcare operation if the covered entities are identified, the locations to which the Notice applies is described and if it states, if applicable, that the covered entities will share PHI for treatment, payment or health care operations; and
h. Company must publish an amended notice at any time a material change has occurred.

2. *Complaints*. Any person, including a patient, may file or make a complaint to the Company and to the Department of Health and Human Services regarding the Company's Notice of Privacy Practices. ***The Company shall not retaliate in any way (e.g., intimidation, threatening behavior, coercion, discrimination, or refusal to treat or continue treatment) against any person who makes a complaint, oral or written, regarding the privacy of patient information.*** If a Patient expresses concern regarding information privacy, direct the Patient to the Privacy Officer. The Privacy Officer should document that complaint, respond in writing acknowledging the complaint, and initiate investigation of the complaint. In the event of threatened litigation or potential liability, involvement of legal counsel and notice to insurer may be necessary. To the extent that an impermissible use or disclosure has occurred, ***Incident Response Plan*** and ***Breach Notification Policy*** should be consulted and initiated. Steps to mitigate any harm or risk to PHI should occur as soon as feasible. If a Business Associate is involved, the Privacy Officer should notify the Business Associate of a complaint made regarding its privacy practices and investigate accordingly. Refer to the BAA for correct notification procedures.

HIPAA Privacy Policy and Procedure No. 11
Incident Response Plan/Business Continuity Plan

Purpose

To describe the Company's response to adverse incidents and other circumstances that pose a threat to the continuity of normal business operations of the Company.

Policy

It is the policy of Company that Workforce must report all unusual and/or suspicious information security-related events in the Protected Data environment. These events may include unusual and troublesome requests for internal information coming from an external party or which appear to be internal, previously unseen dysfunctional system behavior, suspected computer virus infections, erroneous system results, social engineering, and information service failures. All unauthorized access, use or disclosures of Protected Data must be immediately reported to the Privacy Officer and Security Officer.

Incident Response Plan

It is the policy of Company that Workforce must not attempt to deal with security incidents, violations or problems without expert technical assistance. Technical responses to security incidents, violations and problems must be handled exclusively by the Security Officer or the IT vendor and/or others who have been authorized by the Security Officer.

An Incident Response Plan shall be implemented and utilized for all incidents in the Protected Data environment including but not limited to Protected Data breaches.

1. *Computer Security Incident Response Team (CSIRT)*: The Security Officer should identify in advance the Computer Security Incident Response Team (CSIRT). This may include the Security Officer and others in the Company needed to respond in the event of a Security Incident, as well as external experts, such as IT Vendor(s) and legal counsel. The CSIRT is responsible for preparing, maintaining, and periodically testing response procedures to a variety of computer security incidents including denial of service attacks, hacker intrusions, frauds, virus infestations, and power outages.

2. *Incident Reporting*: Each Workforce member is required to report any suspected Security Incident. Security Awareness training shall include information on how to identify suspected instances of Security Incidents. The Incident Reporting Form shall be used. **Workforce shall immediately notify a Supervisor and the Security Officer of a suspected instance of a Security Incident, such as a phishing email, unusual network action, inability to access network, EHR or other software system, or receipt of a ransomware notice.**

3. *Incident Response*: All initial reports of what appears or are suspected to be a security incident must be immediately reported to the Security Officer. The Security Officer will investigate whether an incident actually occurred, the severity of the incident, and the

urgency of a response. All reported incidents that are designated as legitimate incidents will be promptly classified according to their severity and urgency. Incidents may require reclassification as further information comes to light. The Security Officer will decide which methods and processes will be followed in response to an incident. These methods and processes ideally are documented in the Incident Response Plan, but they may also be determined on an ad hoc basis, in response to the needs of the situation. The Security Officer will track all events and tasks associated with the incident, providing status to all appropriate parties. A documented history of all incidents shall be maintained by the Security Officer. If the Incident involves PHI or ePHI, the Breach Notification Policy must also be followed.

4. *Notifying Third Parties*: If a data breach causes private or proprietary third party information to be exposed, then these same third parties must be promptly notified so that they can take appropriate action. All such external notification efforts must be approved by both the Information Security Officer and Legal Counsel. If the Breach is of unsecure ePHI, the procedures set out in the ***Breach Notification Policy*** shall be followed.

5. *System Monitoring*: Company shall monitor its network, systems and devices for Security Incidents and conduct audits**.** Pursuant to the BAA with its IT Vendor, the Vendor shall monitor its systems and give Company notice of a Security Incident as soon as possible.

Business Continuity Plan

Company will develop, adopt and implement a Business Continuity Plan that contains the critical information Company will require to continue business operations and provide care to its patients in spite of adverse events. The Plan must clearly state Company essential functions in writing, identify and prioritize which systems and processes must be sustained, and provide the necessary information for maintaining them. The continuity plan must include the following minimum information:

Employee contact list;
Supplier/vendor information;
Prioritized list of critical business functions;
Recovery locations;
Copies of Essential Records;
Inventory of Company's computer equipment and software;
Data Backup; and
Network Configuration Information.

HIPAA Privacy Policy and Procedure No. 12
Reporting Breaches and Other Impermissible Uses and Disclosures

Purpose

To describe the circumstances under which Practice reports all disclosures of PHI that violate state or federal laws.

Policy

It is the policy of Company to promptly investigate any impermissible use or disclosure of PHI that violates federal laws and regulations, including but not limited to HIPAA and applicable state laws and regulations, initiate mitigation procedures, as appropriate, enforce appropriate sanctions, and report any Breach of PHI that compromises the privacy and security of the PHI in accordance with Company Breach Notification Policy.

Company is committed to complying with the requirements of the Data Breach Notification Regulations in the event that a breach of relevant PHIas defined by HIPAA is detected. To this end, Company will ensure that written policies and procedures regarding breach notification are documented, workforce members are trained on these policies and procedures, and appropriate sanctions against workforce members who do not comply with these policies and procedures are developed and applied appropriately. Additionally, Company will ensure that proper notifications are made to individuals whose PHI has been breached, media outlets and state and federal government entities such as the Department of Health and Human Services ("HHS"), to the extent mandated by HIPAA.

Procedure

1. A breach will be considered to be "discovered" as of the first day on which the breach is known to Company, including a Workforce member or agent, or should have been known to Company if Company had exercised reasonable due diligence. The due diligence requirement means that Covered Entities and Business Associates should have policies and procedures in place to detect and identify breaches, which require coordination among the individuals and departments that are responsible for the physical, administrative and technical aspects of Company's compliance with the HIPAA Privacy and Security Rules.

2. When a Workforce member knows or suspects that a Patient's PHI may have been disclosed in violation of federal HIPAA laws and regulations, state laws and regulations, or any of Practice policies, the Workforce member must immediately notify a supervisor and/or Privacy Officer. If the matter involves a security incident, then the Security Officer will also be notified and the Incident Response Plan followed. Any supervisor receiving such a report will immediately notify the Privacy Officer. There shall be no retaliation against the reporting Workforce member in response to a report made in good faith.

3. The Workforce member will forward to the Privacy Officer a written report of what he or she believes occurred, including a brief description, the date of the incident, the date on which the incident was discovered, and a description of the PHI suspected to have been breached. If the Workforce member is in possession of unsecure PHI, it will be promptly returned to the Privacy Officer.

4. The Privacy Officer will update the Incident Log and, in consultation with the Incident Response Team, will take the following steps in order to determine whether the entity has breached reporting obligations and will complete a Breach Risk Assessment**.**

a. *Determine whether the PHI was secured or unsecured*. If the Privacy Officer determines that the PHI was secured, then he or she updates the Incident Log accordingly and enters the date that the incident was closed. The Privacy Officer will complete the Breach Risk Assessment indicating that the information was secure. If the Privacy Officer determines that the PHI was unsecured, then he or she will proceed to step b. In the event of a ransomware attack that encrypts PHI, OCR presumes a breach.

b. *Determine whether the use or disclosure falls under one of the exceptions to the definition of a breach*. If the Privacy Officer determines that the disclosure meets one of the exceptions, then he or she updates the Incident Log accordingly and enters the date that the incident was closed. If the Privacy Officer determines that the unsecured PHI that was breached does not fall under one of the exceptions to the definition of a breach, then he or she will proceed to step c.

c. *Determine whether there is a "low probability" that the PHI was compromised*. In determining whether there is a low probability that the PHI has been compromised, the Privacy Officer must perform a risk assessment that includes at least the following considerations: (i) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (ii) the unauthorized person who used the PHI or to whom the disclosure was made; (iii) whether the PHI was actually acquired or viewed; and (iv) the extent to which the risk to the PHI has been mitigated. If the Privacy Officer determines that there is more than a low probability that the PHI has been compromised, then a Breach has occurred and notification is required.

4. If the incident meets the definition of a Breach, then the Privacy Officer will provide appropriate notification of the breach in accordance with the Breach Notification Rules.

5. In the event of a breach, the Privacy Officer will complete the following notification requirements:

a. *Individual Notice*

The Privacy Officer will provide 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 Company has insufficient or out-of-date contact information for ten (10) or more affected individuals, the Privacy Officer will provide for substitute individual notice either by 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. Company may choose to do this without waiting for a determination that there are more than ten (10) individuals with incorrect or insufficient contact information.

If Company has insufficient or out-of-date contact information for fewer than ten (10) individuals, the Privacy Officer may provide substitute notice by an alternative form of written, telephone, or other means. If the individual has provided an email, contact by email is permitted.

These individual notifications will be provided without unreasonable delay and in no case later than sixty (60) days following the discovery of a breach and will 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 will include a toll-free number for individuals to contact the Covered Entity to determine if their PHI was involved in the breach.

b. *Media Notice*

If the breach affects more than five hundred (500) patients, in addition to notifying the affected individuals, the Privacy Officer will provide notice to prominent media outlets serving the State or jurisdiction. Like individual notice, this media notification will be provided without unreasonable delay and in no case later than sixty (60) days following the discovery of a breach and will include the same information required for the individual notice.

c. *Notice to the Secretary*

The Privacy Officer will notify the Secretary by filling out and electronically submitting a breach report form on the HHS website:

(http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html)

If a breach affects five hundred (500) or more individuals, the Privacy Officer will notify the Secretary without unreasonable delay and in no case later than sixty (60) days following a breach.

If a breach affects fewer than five hundred (500) individuals, the Privacy Officer may notify the Secretary of such breaches on an annual basis, no later than sixty (60) days after the end of the calendar year in which the breaches occurred.

(http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html)

d. If law enforcement requests a delay in notification, notice or posting on the grounds that it could impede a criminal investigation or cause damage to national security, Company shall delay for the time period requested in the written statement, or if requested orally Company shall document the request and delay notification for no longer than thirty (30) days.

6. In addition to the steps detailed above, following any breach, the Privacy Officer will determine whether the breach implicates additional reporting obligations under applicable state

security breach reporting laws that are not preempted by the Privacy Rule or Security Rule and comply with any such reporting requirements.

Documentation

This version of the policy, together with any forms and other documentation created or obtained in accordance with the policy, will be retained by Company for at least six (6) years from the date of last use or date of creation, whichever is later.

HIPAA Privacy Policy and Procedure No. 13
Uses By and Disclosures to Business Associates

Purpose

To describe the relationship and respective commitments, responsibilities and obligation of Company and any vendors or business associates of Company who use or disclose PHI on behalf of Company.

Policy

Company is required to have in place Business Associate Agreements ("BAAs") with all of its Business Associates who use or disclose PHI on behalf of Company. A BAA establishes the permitted and required uses and disclosures of PHI by the Business Associate or Subcontractor and also authorizes termination of the BAA or other relationship if it is determined that the Business Associate has violated the terms of the agreement.

Definitions

Capitalized terms used but not defined herein shall have the meanings given to them by HIPAA and/or the HIPAA Rules.

Agreements with Business Associates

Practice will identify and maintain a log of all of its Business Associates. At the beginning of a new relationship with a Business Associate, Company will confirm that a BAA is in place and whenever possible, will use one of its templates. Any customer or vendor BAA template must be forwarded to the Privacy Officer for review and, if necessary, negotiation.

The Privacy Officer or his/her designee will sign all BAAs. Copies of all signed BAAs will be kept for a minimum of six (6) years following original signature or the last date the agreement was in effect, whichever is longer.

Required Components. The following items are required elements of a BAA:

(a) Requiring the Business Associate to only use or disclose PHI in accordance with the BAA or as required by law. The services and duties of the Business Associate must either be specified in an underlying service agreement or in the BAA.

(b) Requiring the Business Associate to maintain appropriate administrative, technical and physical safeguards to protect the confidentiality of PHI and to comply with the applicable provisions of 45 CFR Part 164, Subpart C of the HIPAA Rules with respect to Electronic PHI to prevent any use or disclosure of such information other than as provided by the BAA.

(c) Requiring the Business Associate to report non-permitted uses and disclosures, security incidents and breaches of Unsecured PHI.

(d) Requiring the Business Associate to obligate in writing its downstream Subcontractors to comply with the same requirements and conditions that apply to the Business Associate with respect to such information.

(e) Requiring the Business Associate to make PHI available and to amend PHI to satisfy the individual rights provisions of the HIPAA Rules.

(f) Requiring the Business Associate to document disclosures required to be reported under the accounting obligation and to provide such documentation upon request.

(g) Requiring the Business Associate to provide access to its internal practices, books and records to HHS for purposes of determining compliance with the HIPAA Rules.

(h) Requiring the Business Associate to return or destroy all PHI upon termination of the BAA, if feasible, and to continue to abide by the BAA with respect to any PHI that is infeasible to return or destroy and only use and disclose retained PHI for purposes that make return or destruction infeasible.

(i) Authorizing termination of the BAA if the Business Associate violates a material term of the BAA.

(j) Requiring the Business Associate, to the extent that the Business Associate is to carry out an obligation of a Covered Entity under the HIPAA Rules, to comply with the requirements of the HIPAA Rules that apply to the Covered Entity in the performance of such obligation.

(k) Any other items required by the HIPAA Rules, as may be amended from time to time.

The BAA may also expressly address other items such as the minimum necessary standard, restrictions on the use or disclosure of PHI for marketing or fundraising, prohibitions on the sale of PHI and that the Business Associate may be subject to the penalty provisions of the HIPAA Rules.

Oversight of Business Associates

Company will perform reasonable and appropriate reviews of its Business Associates. The scope and frequency of such reviews will vary depending on the nature and extent of PHI being shared with the Business Associate and may involve surveys, obtaining signed certifications and on-site reviews as deemed appropriate by the Privacy Officer (in coordination with the Security Officer for Business Associates/Subcontractors that access or receive electronic PHI).

A Workforce member who becomes aware of any pattern of activity or Company of a Business Associate or Subcontractor that constitutes a material breach or violation of the BAA must promptly notify the Privacy Officer. Company will take reasonable steps to cure the breach or end the violation by the Business Associate. If such steps are unsuccessful, Company shall terminate the agreement between the parties.

HIPAA Privacy Policy and Procedure No. 14
Sanctions

Purpose

To describe the sanctions imposed and other actions taken by Company in the event of a Workforce member's noncompliance with these Policies.

Policy

All Workforce members must comply with the policies and procedures of Company. Company will use appropriate sanctions against Workforce members who fail to comply with these HIPAA Privacy Policies.

Procedures

1. *Disciplinary Actions*. The Privacy Officer, in conjunction with legal counsel and Human Resources, will review all reports of non-compliance and determine the severity of disciplinary actions necessary. Disciplinary actions may range from a verbal warning to termination and will be administered consistent with applicable HR policies. Factors that will impact the disciplinary action adopted include (a) whether the non-compliance was accidental, intentional, and/or malicious; (b) the scope of the violation, including the amount and types of PHI involved; (c) whether the individual has previous instances of non-compliance; and (d) whether the individual attempted to cover-up the violation, was forthcoming or tried to undermine the Privacy Officer's investigation. The unauthorized use or disclosure of PHI may also result in monetary penalties under HIPAA or other civil or criminal penalties

2. *Documentation*. All sanctioning activities will be documented and retained by the Privacy Officer for a period of at least six (6) years from the date of its creation or the date when it was last in effect, whichever is later, in compliance with these policies.

3. *Reports*. Workforce members who become aware of a potential violation of these HIPAA Privacy Policies must report the incident as set forth in these policies. If the Privacy Officer is the subject of the incident report, the workforce member should report the incident to Human Resources or their supervisor simultaneously.

4. *Exceptions*. Company will not apply disciplinary action to the extent the use or disclosure of PHI involves one of the following:

4.1 A whistleblower disclosure made in good faith to a health oversight agency or public health authority with respect to Company's conduct or compliance with the law or to an attorney being retained to represent the person making the disclosure for purposes of determining the legal options of the whistleblower;

4.2 A limited disclosure by a victim of a crime to a law enforcement official, where the disclosure is about the suspected perpetrator of the criminal act and the information disclosed is limited to the information that may be disclosed to a law enforcement official under the HIPAA Rules;

4.3 Filing a complaint with Company and/or HHS;

4.4 Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing concerning the HIPAA Rules;

4.5 Opposing any act or Company that is prohibited by the HIPAA Rules, provided that (i) the person has a good faith belief that the Company being opposed is unlawful; and (ii) the manner of opposition is reasonable and does not itself violate the HIPAA Rules.

5. *Business Associates*. If Company becomes aware of any pattern of activity or Company of a Business Associate or Subcontractor that constitutes a material breach or violation of the BAA with the Business Associate (or the HIPAA Rules), Company will take reasonable steps to cure the breach or end the violation by the Business Associate. If such steps are unsuccessful, Company shall terminate the agreement between the parties. Any Workforce member who becomes aware of a potential or actual breach of a BAA by a Business Associate or Subcontractor or non-permitted use or disclosure of PHI by a Business Associate must immediately notify the Privacy Officer.