ORCHID SURGICAL, LLC

HIPAA PRIVACY POLICIES AND PROCEDURES

ORCHID SURGICAL, LLC
HIPAA PRIVACY POLICIES AND PROCEDURES

Table of Contents

General

Introduction:

It is the policy of Orchid Surgical, LLC ("Company") that all personnel must preserve the integrity and confidentiality of protected health information ("PHI") and other sensitive information pertaining to the patients of our covered entity clients. The purpose of these *Privacy Policies and Procedures* is to ensure Company's compliance with applicable standards, implementation specifications, and requirements of the HIPAA Privacy Rule with respect to PHI. Furthermore, the purpose of these *Privacy Policies and Procedures* is to ensure that Company and its workforce have the necessary medical and other information to provide the highest quality services possible while protecting the confidentiality of that information to the highest degree possible so that covered entities do not fear to provide information to Company and its workforce.

General Policy:

Shonte Amato-Grill shall serve as Company's Privacy Officer. Company and its personnel shall not use or disclose PHI, except as permitted or required by the HIPAA Privacy Rule and the HIPAA Security Rule. All Company workforce members are required to comply with all *HIPAA Privacy Policies and Procedures*. In addition, workforce members are expected to report known or suspected violations of the *HIPAA Privacy Policies and Procedures* by others. Reports of violations should be in writing and directed to Company's Privacy Officer.

Procedures:

1) Company shall only use and disclose PHI in accordance with the appropriate Business Associate Agreements it has entered into with its covered entity clients and any downstream HIPAA Subcontractor Agreements with its subcontractors. In the event that the obligations of Company pursuant to an applicable Business Associate Agreement or HIPAA Subcontractor Agreement conflict with the policies or procedures set forth in these *HIPAA Privacy Policies and Procedures*, Company shall comply with its obligations pursuant to the applicable Business Associate Agreement.

2) Subject to the terms of the applicable Business Associate Agreement or HIPAA Subcontractor Agreement, Company may use PHI for the following purposes:

    a) Use the PHI in its possession as necessary for the proper management and administration of Company or to carry out its legal responsibilities.

    b) Disclose the PHI in its possession as necessary for the proper management and administration of Company or to carry out its legal responsibilities, if:

        (1) Such disclosure is required by law, or

(2) Company obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies Company of any instances of which it is aware in which the confidentiality of the information has been breached.

c) Provide Data Aggregation services relating to the operations of the covered entity if required under any agreement(s) between a covered entity and Company.

3) The Privacy Officer shall conduct an investigation whenever there is a credible allegation that a violation of these *HIPAA Privacy Policies and Procedures* has occurred and shall recommend appropriate sanctions for such violations, if any.

4) When using or disclosing PHI or when requesting PHI from a covered entity, Company will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The foregoing minimum necessary requirement does not apply to the following:
   a) disclosures made to HHS as required to investigate or determine Company's compliance with the HIPAA Privacy Rule;
   b) uses or disclosures that are required by law under the HIPAA Privacy Rule; and
   c) uses or disclosures that are required for compliance with the applicable requirements of the HIPAA Privacy Rule.

Sanctions Policy

General Policy

Whenever there is a credible allegation that a violation of the HIPAA Privacy Rule, HIPAA Security Rule, or Company's HIPAA Privacy or Security Policies has occurred, Company shall investigate the allegation and shall recommend appropriate sanctions for such violations, if any.

Procedures

Sanctions for workforce members may include, but are not limited to: verbal warnings, written warnings, paid and unpaid suspensions, and termination, in accordance with applicable personnel policies.

1. **Definition of a Violation:** The level of breach in patient confidentiality or privacy violation is determined according to the severity of the breach or violation, whether the breach or violation was intentional or unintentional, and whether the breach or violation indicates a pattern or practice of improper use or release of confidential patient information or violation of patient privacy. The degree of discipline may range from a verbal warning to immediate termination.

    a. **Class I Violation(s): Carelessness or Inadvertent action.** This level of breach or violation occurs when a Company workforce member unintentionally or carelessly accesses, reviews, or releases confidential patient information without a legitimate business reason. Examples include, but are not limited to:

        i. Leaving PHI in an unsecured area where it might be viewed by others;

        ii. Leaving a computer unattended while the workforce member is logged on to a system containing PHI;

        iii. Sharing PHI with another workforce member without authorization or unrelated to the performance of the workforce member's duties;

        iv. Discussing PHI in public areas where the workforce member can be overheard (i.e. patient waiting room, restroom, etc.); or

        v. Faxing documents to the wrong location or mailing/giving documents to the wrong person/patient.

    b. **Class II Violation(s): No Personal Gain.** This level of breach or violation occurs when a workforce member intentionally accesses or releases confidential patient information for purposes other than the care of the patient or other authorized purposes but for reasons unrelated to personal gain. Examples include but are not limited to:

        i. The sharing of computer access codes (username & password); or

ii. The use of another person's computer access codes (username & password).

c. **Class III Violation(s): Personal Gain or Malice.** This level of breach or violation occurs when a workforce member accesses, reviews, or releases confidential patient information for personal gain or with malicious intent. Examples include, but are not limited to:

i. Accessing or reviewing a health record of a patient without a legitimate business purpose, such as reviewing the health record of a patient in the news, another workforce member's information, or a public personality.

ii. Using and/or disclosing PHI for commercial advantage, personal gain or malicious harm; or

iii. Obtaining PHI under false pretenses.

2. **Sanctions:** Violation of this policy will result in action appropriate to the circumstances, the class of offense, and whether there is a pattern of repeated violations. The following steps are guidelines for disciplinary action for privacy breaches and violations. Risk to patients or staff and other serious offenses may warrant deviation from these guidelines. Such disciplinary actions may include, but are not limited to, any one or more of the following:

a. Class I Violation(s):

i. First Offense: A documented warning.

ii. Multiple Offenses: Each subsequent Class I Violation constitutes a Class II Violation.

b. Class II Violation(s):

i. First Offense: Depending on the facts, (1) documented warning, and/or (2) final written warning/last chance agreement.

ii. Multiple Offenses: Depending on the facts, (1) final written warning/last change agreement, (2) suspension up to five days without pay, documented and maintained in the workforce member's file, and/or (3) immediate termination with reports to appropriate agencies if applicable.

c. Class III Violation(s):

i. First or Subsequent Offense: Depending on the facts, (1) suspension up to five days without pay, documented and maintained in the workforce member's file, and/or (2) immediate termination with reports to appropriate agencies if applicable.

ii. Civil and criminal penalties as provided under HIPAA and other applicable Federal/State/Local laws.

3. Exceptions: No sanctions or retaliatory actions shall apply to:

a. **Whistleblowers.** Workforce members who believe in good faith that Company has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by Company potentially endanger patients, workers, or the public shall not be sanctioned for disclosing PHI to the following individuals or entities:

i. A health oversight agency or public health authority authorized by law to investigate or oversee the conduct or conditions of Company so long as the purpose of the disclosure was to report the allegation regarding Company's failure to meet the relevant legal or professional standards;

ii. A health care accreditation organization, so long as the purpose of the disclosure was to report the allegation regarding Company's failure to meet the relevant legal or professional standards; or

iii. An attorney retained by or on behalf of the workforce member for the purpose of determining the legal options that the member has with regard to Company's alleged illegal or unprofessional conduct under Section 3.a.

b. **Individuals who oppose actions that violate HIPAA.** Sanctions will not be applied to any individual for the following:

i. Filing a truthful complaint with HHS, or other governmental agency, regarding a privacy violation;

ii. Testifying, assisting, or participating in any official investigation, compliance review, proceeding, or hearing under HIPAA; or

iii. Opposing any act of Company that violates the HIPAA Privacy or Security Rules, as long as the individual doing so believes in good faith that the act of Company is unlawful, and the manner of the opposition is reasonable and does not involve making a disclosure of PHI that violates HIPAA.

Incidental Disclosures of PHI

General Policy:

Incidental disclosures are disclosures of PHI that occur as a by-product of a permissible use or disclosure, are limited in nature, and cannot be prevented through the use of reasonable measures. Incidental disclosures do not violate Company's *HIPAA Privacy Policies and Procedures* as long as: (1) reasonable measures were taken to prevent the incidental disclosure; and (2) the disclosure resulted from a use or disclosure that is otherwise permissible under Company's *HIPAA Privacy Policies and Procedures*, including policies regarding using or disclosing the minimum necessary information.

Procedures:

1) The following measures are considered reasonable with respect to the prevention of incidental disclosures and shall be followed when applicable:
   a) Compliance with the *Policy Regarding Transmission of PHI via Facsimile, Policy Regarding Transmission of PHI via E-mail*, and the *Policy Regarding Transmission of PHI via Telephone* shall constitute reasonable measures for the prevention of incidental disclosures when receiving or disclosing PHI via telephone, e-mail or fax.
   c) When discussing PHI in any non-private area (e.g., reception area or hall), all conversations should be kept as low as reasonably possible. Private areas should be used for such discussions whenever reasonably possible. If PHI is communicated via sign language, reasonable efforts should be made to move the discussion out of plain view of passersby.
   d) Computer screens should be set-up out of view of unauthorized individuals.

Requests from Patients

General Policy:

Under the HIPAA Privacy Rule, patients have certain rights with regard to their PHI, including but not limited to the right to access their PHI, the right to request restrictions on the use or disclosure of PHI, the right to request amendments or corrections to PHI, and the right to request an accounting of disclosures of PHI. Company will cooperate with its covered entity clients to ensure compliance with such patient rights.

Procedure:

1) **Responding to Requests from Covered Entities:** In the event that a covered entity client of Company requests that Company disclose PHI maintained by Company for the purpose of responding to a patient request for: (a) access to PHI, (b) amendment or correction of PHI, or (c) an accounting of disclosures of PHI, Company shall provide the requested PHI to the covered entity. Company must provide the PHI to the covered entity within the timeframe set forth in the appropriate Business Associate Agreement, but no later than the following:

    a. **Request for access to the patient's PHI:** 30 days after Company receives a request from the covered entity;
    b. **Request for amendment or correction of the patient's PHI:** 30 days after Company receives a request from the covered entity;
    c. **Request for an accounting of disclosures of the patient's PHI:** 60 days after Company receives a request from the covered entity. Such accounting of disclosure of the patient's PHI s must include the following: (1) the date of each disclosure, (2) the name of the entity or person who received the disclosure and, if known, the address of that entity or person, (3) a brief description of the information disclosed, and (4) a brief statement of the purpose of the disclosure that would reasonably inform a reader of the basis for the disclosure.

2) **Forwarding Patient Requests:** Except as set forth in the appropriate Business Associate Agreement, Company will forward the following types of requests that Company receives directly from patients to the appropriate covered entity:

    a. Patient requests for access to PHI;
    b. Patient requests for restrictions on the use or disclosure of PHI;
    c. Patient requests for amendment or correction of PHI; and
    d. Patient requests for an accounting of disclosures of PHI.

    Company will not communicate directly with the patient unless specifically directed to do so by the covered entity and the covered entity provides written consent to such communication.

3) **Documentation:** The Privacy Officer is responsible for handling requests from covered entities and patients under this Policy. Company shall retain documentation of the requests for 6 years.

Breach Notification Policy

General Policy:

Company will comply with the federal mandatory breach notification requirements pertaining to the breach of unsecured PHI. To that end, Company will notify covered entities of whom Company is a business associate of a breach of unsecured PHI in accordance with the federal mandatory breach notification requirements. The mandatory reporting obligations set forth in this policy apply only to unsecured PHI.

Definitions:

1) **"Unsecured PHI**" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by HHS.

2) **"Breach**" means, except as provided below, an acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule is presumed to be a breach unless Company or one of its subcontractors, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment which must include at least the factors set forth below in this Policy. The term "breach" does not include:

    a. Any unintentional acquisition, access, or use of PHI by a workforce member of Company or person acting under the authority of Company if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule;

    b. Any inadvertent disclosure by a person who is authorized to access PHI at Company to another person authorized to access PHI at Company, and such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule; or

    c. A disclosure of PHI where Company has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Procedures:

1) **Analysis of Incident.** When determining the probability that a breach has occurred, i.e. whether the privacy or security of a patient's PHI has been compromised, Company shall consider the factors included in the HIPAA Breach Assessment at Exhibit A to this Policy. These factors must include the following:

a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
b. The unauthorized person who used the PHI or to whom the disclosure was made;
c. Whether the PHI was actually acquired or viewed; and
d. The extent to which the risk to the PHI has been mitigated.

Other factors may also be considered as necessary.

2) **Notification.** Company will notify each covered entity whose patient unsecured PHI has been, or is reasonably believed by Company to have been, accessed, acquired, or disclosed because of a breach.

3) **Timing of Notification.** Unless a law enforcement official determines that notification will impede a criminal investigation or cause damage to national security, Company will make the notification required by this policy without unreasonable delay and in accordance with the applicable Business Associate Agreement with Company's covered entity client, and in no event later than sixty (60) calendar days after Company's discovery of the breach. For purposes of this notification timeframe, a breach is deemed to have been discovered on the first day that such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of Company.

4) **Content of Notification.** All breach notices made by Company pursuant to this policy will be written in plain language and will, to the extent possible, include the following information:

a. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

b. A description of the types of unsecured PHI that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, diagnosis, or disability code);

c. The steps patients should take to protect themselves from potential harm resulting from the breach;

d. A brief description of what Company is doing to investigate the breach, mitigate losses, and protect against any further breaches; and

e. Contact procedures for the covered entity to ask questions or learn additional information.

EXHIBIT A: HIPAA BREACH RISK ASSESSMENT

Background Information:	
Date incident occurred	
Date incident discovered by Company's personnel (if different)	
Brief description of the type of information that may have been improperly disclosed or accessed	
Indicate who used or disclosed PHI improperly	
To whom was the information improperly disclosed?	
Does an exception to the definition of "Breach" apply to this situation?	
1. Any unintentional acquisition, access or use of PHI by an Company workforce member	
2. Any inadvertent disclosure of PHI by a person who is authorized to access PHI at Company to another person who is authorized to access PHI at Company	
3. An inadvertent disclosure of PHI in a situation where Company has a good faith belief that the unauthorized person to whom PHI was disclosed would not be able to reasonably retain such information	
Has the individual who improperly acquired or used PHI provided a written assurance that the individual will destroy and/or not further disclose PHI? If so, maintain copies of the signed assurance with this documentation.	
If an exception does not apply, is there a "low probability" that the privacy or security of the PHI was compromised?	
Factor 1: Note the nature and the extent of the PHI involved.	
Factor 2: Indicate who used or disclosed PHI improperly. In addition, indicate to whom PHI was disclosed.	
Factor 3: Was the impermissibly disclosed PHI actually acquired or viewed?	
Factor 4: Was the risk to the PHI mitigated?	

Upon consideration of all factors in combination, Company must evaluate the overall probability that the PHI has been compromised. Unless Company can reasonably establish that there is a low probability that the privacy or security of the PHI was compromised, a breach has occurred and notification is required.

Conclusion:

Signature: _____ Date: _____

Print Name: _____

Privacy Practices Training

General Policy:

Each member of Company's workforce shall be instructed regarding these *HIPAA Privacy Policies and Procedures* and other privacy practices in a manner that is tailored to address the specific functions that the individual receiving that education performs.

Procedures:

1) Training for existing workforce members shall be completed as soon as practicable after these *HIPAA Privacy Policies and Procedures* are adopted by Company. Each individual who joins the workforce after this initial training shall be trained as soon as practicable after joining the workforce.

2) "Workforce" includes all employees, work-study students, volunteers, trainees, and other persons whose conduct is under the direct control of Company, whether or not they are paid employees.

3) Whenever a material change is made to privacy practices, each member of the workforce affected by the change shall be trained regarding the change within a reasonable period of time, as defined by the Privacy Officer.

4) The completion of training required by this *Privacy Practices Training Policy* shall be documented by the individual who offered the training. This documentation shall be retained for at least six (6) years from the date of its creation.

5) The Privacy Officer shall implement and oversee all training required by this *Privacy Practices Training Policy*. To accomplish this task, the Privacy Officer shall have the authority to consult with and delegate authority, as well as appoint committees to develop and perform training activities.

6) If the Privacy Officer believes that a workforce member's failure to attend or participate in the designated training required by this *Privacy Practices Training Policy* is purposeful and not reasonably justified, he or she shall report the information supporting that belief, in writing, and further action shall be taken as may be warranted.

7) Workforce members may be subject to disciplinary procedures for failure to attend and participate in the training required by this *Privacy Practices Training Policy*.

Transmission of PHI via Telephone

General Policy:

Company personnel may release PHI over the telephone in the same manner that such information may be released in person, in accordance with these *HIPAA Privacy Policies and Procedures*.

Procedures:

1) ***Voicemail Services.*** The voicemail system will be password protected to prevent unauthorized access to voicemail messages containing PHI.

2) ***Telephone Directories*.**
   a) Patient telephone numbers shall not be programmed into phones.
   b) Written and computerized directories of patient-contact information will be restricted to authorized individuals only. Employees or any other individual authorized to access patient-contact directories shall not share the information in the directory, in whole or part, with any unauthorized individual.
   c) Computerized directories of patient information shall not remain displayed on a computer screen while not in use.

3) ***Conducting Calls*.** Calls shall be conducted in a manner that preserves patient privacy to the greatest extent possible. Doors, windows, and other partitions should be shut when possible. Care should be taken to limit the volume of one's voice when transmitting PHI, especially if unauthorized individuals are nearby or the information is of a sensitive nature.

4) ***Transmitting Information via Telephone*.** Whenever practical, the individual handling a call that concern PHI shall make efforts to ensure the identity of the caller prior to transmitting PHI. To help ensure the confidentiality of PHI, each incoming caller purporting to be the patient or the patient's representative, when there is doubt as to the identity of the caller, may be asked to state the patient's birth date or address, prior to releasing PHI to the caller.

5) ***Calls to Patients*.** When asking for a patient, information about the clinical condition of the patient shall not be disclosed. This includes not identifying who is calling, if doing so would reveal the patient's condition. If a person at the dialed number states that he or she is the patient, that representation shall be considered confirmation that the patient is the person speaking. PHI may then be discussed with that person.

6) ***Messages for Patients*.** Messages for patients shall be limited to the following:
   a) The name of the person for whom the message is being left;
   b) A request that the patient return the call;

c) Adequate identification of the person placing the call, but only if doing so will not reveal the clinical condition of the patient;
d) The name of the individual for whom the patient may ask for when returning the call, if applicable;
e) The telephone number where the call may be returned; and
e) Whether or not the appointment requires special instructions, but only if doing so will not reveal the clinical condition of the patient.

Transmission of PHI via E-mail

General Policy: Unencrypted e-mail messages may be read by someone other than the intended recipient(s) of the e-mail. In accordance with Company's HIPAA Security Policies, Company's workforce must take the appropriate steps to limit sending unencrypted e-mails with PHI. At a minimum, workforce of Company must comply with the following procedures set forth in this policy when sending PHI to patients via e-mail.

Procedures:

1. Workforce must exercise a greater degree of caution in transmitting PHI electronically than they take with other means of communicating PHI (e.g., written memos, letters, pictures, or phone calls) because of the reduced human effort required to redistribute information electronically.

2. PHI should never be transmitted or forwarded to outside individuals or companies not authorized to receive such information and should not be sent or forwarded to other employees inside the organization who do not have a need to know such information.

3. Workforce must use care in addressing e-mail messages to patients to ensure that messages are not inadvertently sent to unintended recipients.

4. All e-mails containing PHI sent from Company must include the following standard disclaimer:

   This e-mail and its attachments may contain protected health information intended solely for the use of Orchid Surgical, LLC and the recipient(s) named above. Due to the unsecured nature of unencrypted e-mail, the recipient(s) named above understand and agree that there may be some level of risk that the information in this e-mail could be read by a third party. If you are not the intended recipient, you are hereby notified that any review, dissemination, distribution, printing or copying of this email message and/or any attachments is strictly prohibited. If you have received this transmission in error, please notify Orchid Surgical, LLC at Contact@OrchidSurgical.com and permanently delete this e-mail and any attachments.

Transmission of PHI via Facsimile

General Policy:

Company has adopted this policy to comply with the HIPAA Privacy Rule, as well as our duty to protect the confidentiality and integrity of confidential medical information as required by law. PHI shall be transmitted by facsimile only when other means of transmission are not feasible. Minor inconvenience shall not constitute infeasibility. All personnel must strictly observe the standards and procedures set forth in this *Transmission of PHI via Facsimile Policy and Procedure* relating to facsimile communications of patient medical records.

Assumptions:

- Company and the personnel or organizations with which Company does business often will have a need to transmit or receive confidential medical information by facsimile rather than by a slower method, such as mail.
- Personnel may send faxes to unauthorized recipients, faxes may be intercepted or lost in transmission, or Company may not receive a fax intended for it because of one of these or other reasons.
- Thus, the potential for breach of patient confidentiality exists every time someone uses such information.

Procedures:

1) Company, its contracted officers, agents, and employees will send health information by facsimile only when the original record or mail-delivered copies will not meet the needs of immediate patient care.

2) Personnel may transmit health records by facsimile only when urgently needed for patient care or required by a third-party payer for ongoing certification of payment for a patient.

3) Personnel must limit information transmitted to that necessary to meet the requester's needs.

4) Except as authorized by law, a properly completed and signed authorization must be obtained from the covered entity before releasing patient information to a third party who is not the covered entity. Note, that such authorization is not required if directed by covered entity to disclose patient information for treatment, payment or healthcare operations.

5) Personnel may not send by fax especially sensitive medical information, including, but not limited to, AIDS/HIV information, mental health and developmental disability information, alcohol and drug abuse information, and other sexually transmissible disease information without the express authorization of the Privacy Officer.

6) The cover page accompanying the facsimile transmission must include the following confidentiality notice:

This facsimile and its enclosures may contain protected health information intended solely for the use of Orchid Surgical, LLC and the recipient(s) named above. Due to the unsecured nature of facsimiles, the recipient(s) named above understand and agree that there may be some level of risk that the information in this facsimile could be read by a third party. If you are not the intended recipient, you are hereby notified that any review, dissemination, distribution, printing or copying of this facsimile and/or any enclosures is strictly prohibited. If you have received this transmission in error, please notify Orchid Surgical, LLC at Contact@OrchidSurgical.com and shred the facsimile and its enclosures.

7) Personnel must make reasonable efforts to ensure that they send the facsimile transmission to the correct destination. Personnel must pre-program frequently used numbers into the machine to prevent misdialing errors. For a new recipient, the sender must verify the fax number before sending the facsimile and verify the recipient's authority to receive confidential information.

8) Fax machines must be in secure areas, where visitors and patients cannot easily access them.

9) Office personnel are responsible for ensuring that incoming faxes are properly handled, not left sitting on or near the machine, but rather are distributed to the proper recipient expeditiously while protecting confidentiality during distribution.

10) Personnel must report any misdirected faxes to the Privacy Officer.

11) Users must immediately report violations of this policy to their department manager and to the Privacy Officer.

Complaint and Grievance

General Policy:

Company will continually strive to improve the quality of the services it provides and will provide a process for handling complaints and grievances related to the use or disclosure of PHI.

Definitions:

1) ***Complaint:*** an oral concern about compliance with health-information privacy laws.

2) ***Grievance:*** a written concern about compliance with health-information privacy laws and regulations.

3) ***Responsible Party:*** all employees and personnel of Company.

Procedures:

1) All grievances regarding privacy policies and practices, and compliance with those policies and practices, will be accepted and considered. Complaints should be made in writing using the Compliant and Grievance form attached at the end of this *Compliant and Grievance Policy and Procedure* and directed to the Privacy Officer.

2) All grievances will be responded to in writing if the complaint seeks a response.

3) Individuals who file a grievance will not be retaliated against in any way, including through coercion, harassment or refusal of treatment. Violations of this anti-retaliation policy will be handled in accordance with the *Policy Regarding Sanctions for Privacy Violations*.

4) Procedure for Responding to a Complaint:
   a) The Privacy Officer, or his designee, shall review all complaints within a reasonable period but in no event not later than thirty (30) days.
   b) If the complaint seeks a response, and provides contact information, the Privacy Officer (or his or her designee) shall prepare and deliver a written response to the individual who lodged the complaint.
   c) If the complaint does not seek a response, or does not provide contact information, the Privacy Officer (or his designee) shall prepare a written statement of any action taken with regard to the complaint. That statement shall be attached to, and filed with, the complaint.

COMPLIANT AND GRIEVANCE FORM

PERSON WITH COMPLAINT

Date of Report:
Person Reporting:
Home Address:

Telephone #:

Date of Occurrence:
Name & Account # of Patient:
Do you feel the problem involves:
- Accidental disclosure ☐
- Deliberate disclosure ☐
- Other security incident ☐

When did you first become concerned with this issue?

Have you discussed this problem with anyone? Yes No Who? When?

Please state the problem in your own words, giving as much specific information as possible (use back of sheet if you need more space)

Signature: Date:

PERSON TAKING REPORT

Name of person taking report: Position/Title:

Date:

Have you personally interviewed the complainant? Action Taken & Date:

Additional Comments: Follow-up Information & Date:

Business Associate and Subcontractor Agreements

General Policy:

Company will enter into a HIPAA Business Associate Agreement with each of its covered entity clients for which Company provides services that involve Company's creation, receipt, maintenance, or transmission of electronic PHI (ePHI) on the covered entity's behalf.

To the extent that Company is the business associate of its covered entity clients, Company, in accordance with the HIPAA Privacy Rule and HIPAA Security Rule, may permit a subcontractor to create, receive, maintain, or transmit electronic PHI (ePHI) and to use or disclose PHI on Company's behalf only if Company obtains satisfactory assurances, in accordance with this *Business Associate and Subcontractor Agreements Policy and Procedure*, that the subcontractor will appropriately safeguard the information.

Procedures:

1) Company will document the satisfactory assurances required by this Policy through (a) a written Business Associate Agreement with each of its covered entity clients, and (b) a written HIPAA Subcontractor Agreement with each its subcontractors to whom Company delegates certain services or activities requiring the use or disclosure of PHI. It is Company's policy to use its own Business Associate and HIPAA Subcontractor Agreement templates. However, in some instances, Company may accept the contract templates of a covered entity or subcontractor, provided it has reviewed the contract for compliance with HIPAA.

2) If Company knows of a pattern of an activity of the subcontractor that constitutes a material breach or violation of the subcontractor's obligation under the HIPAA Subcontractor Agreement, Company will take reasonable steps to cure the breach or end the violation, as applicable. If such steps are not successful—

   - Company shall terminate the contract or arrangement, if feasible; or
   - If termination is not feasible, Company shall report the problem to HHS.

3) If Company violates the satisfactory assurances it provided as a business associate of a covered entity client, Company will be in noncompliance with the HIPAA Security Rule and this Policy.