State Hill SurgiCenter
HIPAA Compliance Plan

Table of Contents

Introduction and Background

State Hill SurgiCenter is located in Wyomissing,PA0. The Center's medical, administrative and clinical staff place significant emphasis on the importance of compliance with federal and state regulations that apply to covered entities. This plan is an effort to comply with the privacy, electronic transaction and security provisions of the Health Insurance Portability and Accountability Act (HIPAA), which was signed into law in August of 1996.

HIPAA required the Department of Health and Human Services (DHHS) to adopt regulations establishing national uniform standards for the privacy of medical records and other personal healthcare information or protected health information (PHI). Covered health entities must be in compliance with the privacy rule by April 14, 2003. Covered entities include health plans, health care clearinghouses, and health care providers who transmit any health information in connection with a HIPAA standardized electronic transaction, such as claims processing.

Covered entities must comply with the standards for electronic transactions by October 16, 2002 (October 16, 2003 if an extension is filed with CMS by October 15, 2002). The HIPAA security standards final rule was published in the February 20, 2003 Federal Register. Covered entities must comply with the security standards final rule by April 21, 2005.

HIPAA imposes penalties for violation of the rule—civil penalties of $100 per person for unintentional disclosure, criminal fines of up to $50,000 and imprisonment of up to a year for intentional disclosure. Penalties for failure to comply with the standards for electronic transactions may include exclusion from participation with Medicare.

This compliance plan was developed based on:

- The final privacy rule published by the Department of Health and Human Services on August 14, 2002
- The final rule for standard electronic transactions published by DHHS on August 17, 2000
- The final security standards rule published on February 20, 2003

Standards for Electronic Transactions

HIPAA regulations for standard electronic transactions were published in the Federal Register on August 17, 2000 and compliance with these regulations became effective October 16, 2003. The Final Rule adopting changes to the HIPAA electronic transactions and code set standards was published in the Federal Register on February 20, 2003. This final rule modifies a number of the electronic transactions and code sets adopted as national standards under HIPAA, and eliminates the NDC code set as the standard for all providers except retail pharmacies.

These standards apply to any health information that is transmitted in electronic form. HIPAA requires that certain healthcare transactions sent or received electronically must be in a standard format.

HIPAA identifies these healthcare transactions as shown on the list below.

- Health claims or similar encounter information
- Eligibility for a health plan transaction
- Referral certification and authorization
- Health claims status
- Enrollment and disenrollment in a health plan
- Health care payment and remittance advice
- Health plan premium payments
- Coordination of benefits information

Privacy Standards

The privacy rule protects individually identifiable health information transmitted or maintained in any form or medium (electronic, paper, or oral). The rule establishes national uniform privacy standards including:

1. *Restrictions on use and disclosure of protected health information:* a written authorization requirement with exceptions for generally accepted uses and disclosures.

2. *Patient notice requirements:* a requirement that health care providers provide a notice of their privacy practices and requirements designed to provide an "initial moment" for discussions with patients regarding their privacy practices.

3. *Other patient rights related to their protected health information including rights to:*

    - Inspection and copying
    - Amendment of erroneous or incomplete information
    - Confidential communications
    - Accounting of disclosures
    - Submission of complaints

4. *Administrative requirements:* including requirements to appoint a privacy officer, conduct workplace training, to establish policies and procedures, and to document compliance.

The privacy rule indirectly affects business associates of covered entities such as third party billing services, collection agencies, etc. Covered entities must bind their business associates to comply with privacy rule standards.

The privacy rule establishes minimum requirements—a "floor." Physicians must still comply with other state privacy laws that impose more stringent standards. Other privacy laws and regulations impacting Pennsylvania physicians include:

- Physician licensing regulations (records maintenance, confidentiality, and access requirements)
- Hospital regulations (records maintenance, confidentiality, and access requirements)
- AIDS law (confidentiality requirements for HIV-related information)
- Drug and alcohol abuse treatment regulations (confidentiality requirements for patient records of federally-assisted drug and alcohol abuse treatment providers)
- Mental Health Procedures Act (confidentiality requirements for inpatient mental health treatment and involuntary outpatient mental health treatment)
- Judicial code (access requirements and limitations on copying and related charges)

Security Standards

HIPAA regulations also address security requirements that covered entities must include in their operations to assure that electronic information that pertains to patients/ individuals remains secure. Covered entities are required to comply with the security standards rule by April 21, 2005.

The security requirements are divided into the following areas with regards to data integrity, confidentiality, and availability of patient identifiable health information:

- Administrative procedures – documented, formal practices to manage the selection and execution of security measures to prevent, detect, contain, and correct security violations, including the conduct of personnel in relation to the protection of data.

- Physical safeguards – limiting physical access to electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed.

- Technical security services – allowing access to electronic information systems containing protected health information only to those persons or software programs that have been granted access rights.

Guiding Principles

1. State Hill SurgiCenter believes that all patients have a fundamental right to the privacy of their health information. The Center is aware that there has been increasing public concern about potential invasions of patient privacy.

2. State Hill SurgiCenter supports the need for the implementation of policies and procedures to ensure that a patient's privacy is protected and that all health information remains secure.

3. State Hill SurgiCenter will interact with our patients in such a way as to ensure they understand the measures we are taking to ensure that their privacy is being protected. We believe it is the Center's responsibility to educate its patients regarding privacy issues, in addition to ensuring them the protections and rights provided to them under the law.

4. State Hill SurgiCenter believes patients have a right to have their complaints about privacy and/or our privacy and security policies and procedures handled in an effective and efficient manner. We will ensure that any known injury resulting from a violation of the privacy and security standards and/or our privacy and security policies and procedures will be mitigated to the extent practicable. The Center will document all complaints and their disposition.

5. State Hill SurgiCenter will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

- any individual who exercises any right established under the privacy standards;
- any person who complains to the Secretary of Health and Human Services or assists in an investigation, compliance review, or HIPAA enforcement proceeding; or
- any person who opposes any activity on the good faith belief that it violates a privacy standard.

6. State Hill SurgiCenter will not require a patient to waive, as a condition of treatment, his or her rights to complain to the Secretary of Health and Human Services or any other right established under the privacy standards.

7. All Center personnel are subject to the HIPAA compliance plan. Continued association with the Center is dependent upon the lawful conduct of its staff with respect to HIPAA. Each employee must be open and honest in his or her dealings with our patients.

Privacy/Security Officer and Implementation Team

Privacy/Security Officer

Sate Hill SurgiCenter has identified Patricia Hause as its HIPAA privacy and security officer. Patricia Hause will coordinate the Center's HIPAA implementation plan and serve as the contact person for all privacy and security issues.

Patricia Hause will oversee the development and implementation of the Center's privacy and security principles, policies, and practices. She will monitor the organization's services and systems to ensure meaningful privacy and security practices. She will also be responsible for educating and training employees, conducting privacy and security audits, and serving as the liaison with patients and outside entities.

Patricia Hause will also provide quarterly updates to the governing board on the status of HIPAA compliance efforts. Additionally, she will provide information to the governing board regarding any problems associated with the implementation of HIPAA requirements within the Center.

Attachment A is a job description for the Center's privacy and security officer.

Implementation Team

HIPAA implementation is a team effort. State Hill SurgiCenter recognizes that all physicians and employees of the Center must be involved in this process, with the privacy and security officer serving as the leader for these efforts.

The HIPAA implementation team includes representatives from the following areas of the Center.

- Patricia Hause - Business Administrator (Privacy Officer)
- Toni Stefanucci RN, BSN –Clinical Director
- Bonnie Seidel – receptionist
- Sue Endy, RN – Pre-op

Team members will assist with the evaluation of procedures within their areas of the Center relative to the HIPAA privacy and security standards on an ongoing basis. They will assist with determining any necessary changes to these procedures. Team members will also assist with the implementation of new or revised policies and procedures in their areas of the Center.

Review of Information Systems

A review of the information systems containing patient information was performed by the Center. State Hill SurgiCenter utilizes the Centricity software for patient scheduling and billing. Centricity has notified the Center it is compliant with the with the ANSI X12N version 4010 format for claims submission. The State Hill SurgiCenter contracts with etactics for some of the facility claims billing.

- Because The Reading Hospital and Medical Center and etactics require access to PHI to provide software support services to the Center, they will be required to sign a business associate agreement.

- State Hill SurgiCenter utilizes passwords and unique user identification numbers to access the Centricity system. The Center does not limit access to the system, as all individuals who utilize the computer system need access to all of the information in the system for scheduling and billing purposes.

- Back-up tapes for the Center's computer system are made each day by The Reading Hospital and Medical Center.

- A disaster recovery plan is in place that includes contingency plans in the event of a computer systems failure.

- In the future, should the Center decide to discard of any computer hardware, all PHI stored on the hard drives or servers will be destroyed prior to disposal.

- All computer terminals located in public areas of the Center have been equipped with either full-sided monitor visors or privacy screens. The Center has a written policy regarding computer terminals.

- Currently, one individual has access to the computer system via home computer. The access is utilized by a dial-up connection to the system. No Internet connections are available for use presently. The dial-up assures that all information accessed is protected. If the user works with sensitive information, a shredder will be available. Similarly, if sensitive information will be stored in paper form, suitable protection from discovery by unauthorized persons must be available. Remote access to the Center's computers and networks will require that all users be definitively authenticated with fixed passwords or other identification systems approved by the Center's Administrative Director. All remote users will be required to connect to the Center's computers and internal net works via authorized communications systems such as firewalls and modem pools. Inbound connection to the Center's computers or networks through an office desktop modem will be prohibited unless specific approval has been obtained from the Administrative Director. Outbound connection to third party networks including the Internet is permissible through office desktop modems or other types of modems but does not obviate the need to comply with other security precautions related to file downloads and transfers. Leaving personal computer-linked modems in auto-answer mode will be prohibited unless a remote user identification system approved by the Administrative Director has been installed.

- The Center has implemented a system for shredding of written documents containing PHI. There is one shredder in the reception/business office.

- The Center does not communicate with patients using email. Should this situation change in the future, State Hill SurgiCenter will ensure that it complies with the HIPAA requirements relating to encryption.

- Each area within the Center will utilize the prescribed fax format. State Hill SurgiCenter has developed a consistent procedure and format for faxing all information from the Center. The Center's fax cover sheet contains a headline reading "CONFIDENTIAL HEALTH INFORMATION ENCLOSED." Below the header a statement reading as follows is included:

  > "Healthcare information is personal and sensitive information. It is being faxed to you after appropriate authorization from the patient or under circumstances that do not require patient authorization. You, the recipient, are obligated to maintain it in a safe, secure, and confidential manner. Re-disclosure without additional patient consent or as permitted by law is prohibited. Unauthorized re-disclosure or failure to maintain confidentiality could subject you to penalties described in federal and state law."

- All fax machines are placed in areas that are out of public view. All faxes received by the Center will be placed in a secure and confidential location.

- Sate Hill SurgiCenter will verify numbers for all faxes containing PHI that are sent by the Center.

Review and Analysis of Current Procedures

Gap Analysis—Review of Current Processes

A review of the functional areas of the Center was performed to identify current procedures that include the disclosure of protected health information (PHI)-- written, oral, or electronic. The purpose of the review was to determine where and how PHI is disclosed and whether such disclosures are restricted under the HIPAA privacy rules.

The functional areas reviewed included:

- Front Office (patient scheduling, check-in, and check-out)
- Medical records
- Human resource management
- Billing/patient accounts

An analysis was then conducted to identify the gaps between State Hill SurgiCenter current processes and procedures and the requirements of the HIPAA privacy and security standards. The gap analysis is documented below.

Front Office

- Patients check in at the reception desk. At the time of check in, the receptionist verifies some of the demographic information such as phone number, address, etc. with the patient. The information may be provided to the patient in writing to review and make changes rather than reading it out loud to them for verification.

- The Center does not utilize a sign-in sheet. Patients are called by their first name (generally) when it is time for them to be escorted to clinical area of the facility. The patient's ID is then verified with the patient by confirming first and last name and date of birth.

- Scheduling is performed by the front desk staff of the Carim Eye & Retina Center. Because of the sliding glass window, it is difficult for anyone in the waiting room to overhear appointments being scheduled by telephone. Follow-up appointments are scheduled in advance with physician Center staff. Patients are discharged from the recovery area of the facility.

- The Center performs post-procedural phone calls for all patients that do not have a one day post-op appointment. Detailed messages will not be left on patients' answering machines. The Center will simply indicate that the facility has called and to contact the facility or their respective physician practice should there be any questions or concerns. In the event that a post-procedural call cannot be completed, a card will be sent to the patient's home indicating that a call was attempted. The cards are placed in envelopes.

- All consultations are held in a private room. A physician can request that a patient's family be asked to proceed to the consultation room in order to discuss the procedure and other important information.

- The Center will have patients sign a form identifying individuals who may be provided with information regarding their medical care.

- Physicians and staff make every effort to protect PHI by ensuring that conversations with or about patients that occur in the reception area and all areas of the Center are as confidential as possible. The Center has a written policy that addresses this issue.

- State Hill SurgiCenter contacts patients to inform them of their test results. Messages providing detailed information will not be left on answering machines. The Center has developed a written policy defining how these calls will be handled. Test results are also communicated to the individual physician practices. Test results will not be sent to patient via the mail.

- The Center does not post patient schedules in public areas. The staff has reviewed the need to refer to daily schedules (such as at the front desk, nurses' station, etc.) and has placed them in folders so they cannot be viewed by other patients or the general public.

- The Center has written procedures for its functional areas, including check-in, check-out, scheduling, billing, collections, telephone protocols, transcription, opening of mail, handling of medical records, and handling of patients in the clinical areas.

Medical Records

- Medical records are filed in the medical records room. The charts at the front desk area are not accessible to the general public. A staff member always escorts patients to the clinical area. There is therefore little risk that they would have the opportunity to see the names on any medical record.

- The placement of patient charts for various purposes was reviewed during the gap analysis. In all instances where patient records are in use for various purposes, State Hill SurgiCenter makes every effort to ensure that other patients and the general public do not have access to the charts or to the names on the charts.

- The Center currently does not charge patients for copies of their medical records. However, the Center does have a policy that outlines a fee schedule for copying medical records should the Center determine that a charge would be required for copying medical records. The fee incorporates labor, equipment, and supply costs related to the copying as identified in the HIPAA legislation. Patients are provided with an explanation of the fees when they request copies of their medical records. The Center has 30 days to comply with a written request for copies of a patient's medical record. For records stored off site, the Center has 60 days to comply.

- **State Hill SurgiCenter** will comply with the HIPAA regulations by permitting patients to review their medical records on site. The patient will be requested to submit the request in writing. The Center will set up a time that is mutually convenient for the Center and the patient for the patient to review the record. An employee will be present while the patient reviews their record. The Center has 30 days to comply

with such a request if the patient's record is maintained on site. For records stored off site, the Center has 60 days to comply with such requests.

- The Center complies with the HIPAA regulations regarding patients' requests to amend their records. The HIPAA rule permits a physician to deny a request for an amendment if the physician determines that the information in the record: 1) is accurate and complete; 2) was not created by the physician; 3) is not part of the health information maintained by the physician; or, 4) is not part of the information that the patient would be permitted to inspect and copy. The Center has 60 days to comply with a written request by a patient to make an amendment to their medical record.

- Patient medical records are not transported to any other location.

- State Hill SurgiCenter will not be storing any medical records at an off site location.

- All transcription services will be completed by Center staff.

- State Hill SurgiCenter has developed policies and procedures relating to the use and disclosure of PHI. This includes guidelines for determination of the minimum amount of confidential information required to accomplish the intended purpose of each use/disclosure.

Human Resource Management

- State Hill SurgiCenter will incorporate language into its position descriptions regarding the employee's obligation to comply with HIPAA requirements in performing their duties. The language will read, "Employee will carry out all duties and responsibilities in compliance with the HIPAA requirements. Employee will follow all of State Hill SurgiCenter policies and procedures, including those pertaining to HIPAA. Employee will participate in HIPAA and other training programs provided by the Center. Employee will maintain confidentiality in all matters pertaining to patient care."

- The Center has a policy regarding confidentiality in its employee manual. Any violation of the policy constitutes grounds for immediate dismissal. The Center identifies employee sanctions for violation of a patient's privacy (intentional or unintentional).

- All employees will attend HIPAA awareness training, at minimum. All training will be documented by the Center, as noted in a later section of this compliance plan.

- The Center has procedures in place to ensure that when an employee terminates employment with the facility; all keys are returned as well as other items that allow both computer and physical access to protected health information. These procedures are specified in the employee manual

Billing and Patient Accounts

- The Center will require Berks Credit and Collections, a collection agency, to sign a business associate agreement.

Implementation Plan

Policies and Procedures

In developing policies and procedures, the State Hill SurgiCenter has addressed key issues such as whether the proposed solutions were reasonable and justifiable from an expense standpoint. Additionally, the Center has assessed whether the policies and procedures are patient-friendly and whether they are workable for the other entities with which State Hill SurgiCenter exchanges PHI.

State Hill SurgiCenter will amend its policies and procedures as needed to comply with any changes in the law. These changes will be documented through revisions to any existing forms and manuals and will be distributed to all individuals that are impacted by the changes. This may include staff, physicians, patients, business associates and other entities.

Policies and procedures have been tested prior to implementation. Staff from various areas of the Center will be involved in developing policies and procedures that are most relevant to their particular job duties in the future.

Implementation of HIPAA Compliant Forms

The Center will provide a notice of privacy practices to its patients. Other HIPAA compliant forms have been developed and are provided in the forms and notices section of this compliance plan.

Business Associates

Business associates are defined as “a person [or entity] who acts in a capacity other than as a member of the workforce of a facility to perform or assist in the performance of a function or activity involving the use or disclosure of confidential information, or any other function or activity otherwise governed by the privacy regulations.”

State Hill SurgiCenter is obligated, under HIPAA regulations, to obtain satisfactory assurance that all business associates will:

- not use or further disclose the information other than as permitted under contract or as required by law
- use appropriate safeguards to prevent use or disclosure of the information other than as provided by the contract
- report to the Center any use or disclosure not provided for by the contract of which it becomes aware
- ensure that any agents to whom it provides confidential information agree to the same restrictions on the information as the business associate
- allow individuals to access their information as required under HIPAA
- make information available for amendment and incorporate amendment
- make available information to provide an accounting of disclosures
- make any confidential information provided by the Center available to the Secretary [of DHHS] for purposes of assessing the Center’s compliance
- return or destroy all confidential information received from the Center at the termination of the contract

State Hill SurgiCenter examined its relationships with outside persons/entities. Those that are considered to fit the description of “business associates” or “contact business associates” will be issued HIPAA business associate contracts or confidentiality agreements to sign. Contact business associates are entities that do not need access to PHI but will likely come in contact with PHI while performing services for the Center.

The Center’s business associates include:

- The Reading Hospital and Medical Center
- Berks Credit and Collection Agency
- Zirmed

The Center’s contact business associates will be asked to sign confidentiality agreements. They include:

- Ron Olesnavich – Alcon
- Kevin Rhodes – Alcon
- Drew Wagner - Optovision
- Coverall North America, Inc

All signed contracts will be placed on file in the office of the Clinical Director.

Education and Training

All physicians, non-physician practitioners, and facility staff will be appropriately trained on HIPAA standards. HIPAA requires that ***all*** members of the workforce be adequately trained in the areas that affect their respective job functions.

Initial awareness training was provided to all current staff prior to state licensure on July 23, 2008. More detailed training may be required for the various functional areas of the Center and will be provided as needed.

Additional education will be provided when new developments occur or when any material changes to the Center's policies and procedures are implemented. Ongoing training sessions will occur periodically.

All training is appropriately documented. Documentation includes the content of the training session as well as the signature of all attendees. Attachment B is a training record form that can be utilized by the Center to record the training sessions. All training records will be located in the office of the facility administrator.

New employees and physicians will be trained within 30 days of joining the Center.

Forms and Notices

State Hill SurgiCenter has implemented the use of certain forms and notices which are included in this section of the plan. The forms will be revised as needs dictate and include the following:

- **Notice of Privacy Practices** - a document that informs patients of the possible uses and disclosures of confidential information, their individual rights, and the Center's legal duties with respect to confidential information. A copy of the Center's notice will be given to each patient on the date of the first service delivery or as soon as reasonably practicable. A copy of the Center's notice will also be posted in the waiting area.

- **Acknowledgement of Receipt of Notice** – a form signed by the patient or the patient's personal representative to indicate that a copy of the Center's notice of privacy practice was received. The Center will have all patients sign the acknowledgement when the notice is distributed and the signed form will be placed in the patient's medical record.

- **Good Faith Efforts to Obtain Acknowledgement** – a form to document a patient's refusal to sign an acknowledgement of receipt of notice form. The Center will document any patient's refusal to sign or accept a copy of the Center's notice. This documentation will be placed in the patient's medical record.

- **Authorization** – a form used for patients to provide the Center with written permission to use or disclose PHI for reasons not specified in State Hill SurgiCenter notice of privacy practices. Examples include, but are not limited to requests from the patient's attorney, life insurer, or employer. The Center will obtain authorization from the patient and a copy of the signed authorization will be placed in the patient's medical record.

- **Re-disclosure Notices** – a notice required with certain disclosures informing the patient that re-disclosure of confidential information is restricted. The Center will include these notices with disclosures of confidential information when necessary.

- **Accounting of Disclosures** – a log utilized to document disclosures of PHI that are not for treatment, payment, or health care operations purposes, or where there is no signed authorization. Examples include mandatory reporting and other public policy disclosures not requiring authorization. This log will be placed in the patient's medical record so that an accounting of disclosures can be provided upon request.

- **Business Associate Agreement** – a contract between the Center and an individual or entity that is required to have access to the Center's PHI in order to perform services to or on behalf of the Center. The Center will issue a business associate agreement to ensure the protection of confidential information.

- **Confidentiality Agreement** – a contract between the Center and an individual or entity that may have incidental access to the Center's PHI in order to perform services for the Center. The Center will issue a confidentiality agreement to ensure the protection of confidential information.

Notice of Privacy Practices

NOTICE OF PRIVACY PRACTICES FOR
STATE HILL SURGICENTER

Effective date: July 1, 2008

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

If you have any questions regarding this notice, you may contact our privacy officer at:

Address: 2630 Westview Drive
Wyomissing, PA 19610
Telephone: 610-898-1515
Facsimile: 610-898-1525

I. YOUR PROTECTED HEALTH INFORMATION

State Hill SurgiCenter is required by the federal privacy rule to maintain the privacy of your health information that is protected by the rule, and to provide you with notice of our legal duties and privacy practices with respect to your protected health care information. We are required to abide by the terms of the notice currently in effect.

Generally speaking, your protected health information is any information that relates to your past, present or future physical or mental health or condition, the provision of health care to you, or payment for health care provided to you, and individually identifies you or reasonably can be used to identify you.

Your medical and billing records at our Center are examples of information that usually will be regarded as your protected health information.

II. USES AND DISCLOSURES OF YOUR PROTECTED HEALTH INFORMATION

A. Treatment, payment, and health care operations

This section describes how we may use and disclose your protected health information for treatment, payment, and health care operations purposes. The descriptions include examples. Not every possible use or disclosure for treatment, payment, and health care operations purposes will be listed.

1. Treatment

We may use and disclose your protected health information for our treatment purposes as well as the treatment purposes of other health care providers. Treatment includes the provision, coordination, or management of health care services to you by one or more health care providers. Some other examples of treatment uses and disclosures include:

- We will call you by name from the waiting room when it is time for you to go to the preparation area for your procedure.

- We may leave messages on your answering machine or send cards regarding follow-ups to your procedure or to request that you contact us to discuss your test results.

2. Payment

We may use and disclose your protected health information for our payment purposes as well as the payment purposes of other health care providers and health plans. Payment uses and disclosures include activities conducted to obtain payment for the care provided to you or so that you can obtain reimbursement for that care, for example, submission of a claim form to your health insurer.

3. Health care operations

We may use and disclose your protected health information for our health care operation purposes as well as certain health care operation purposes of other health care providers and health plans. Some examples of health care operation purposes include:

- Quality assessment and improvement activities
- Health care fraud and abuse detection and compliance programs

B. Uses and disclosures for other purposes

We may use and disclose your protected health information for other purposes. This section generally describes those purposes by category.

1. Individuals involved in care or payment for care - such as a spouse, a family member, or a close friend. For example, when you have a procedure, we may discuss your physical limitations with a family member or other individual assisting in your care. We may discuss your care only with individuals who you have identified by verbal or written consent.

2. Notification purposes - to notify a family member, a personal representative, or another person responsible for your care, regarding your location, general condition, or death.

3. Required by law or law enforcement purposes - when required by federal, state, or local law. For example, we may disclose protected health information in response to a court order or subpoena.

4. Public health activities - For example, filing communicable disease reports with public health agencies.

5. Business associates - certain functions of the Center performed by a business associate such as a consulting firm, an accounting firm, or a law firm. We may disclose protected health information to our business associates and allow them to create and receive protected health information on our behalf. For example, we may share with our attorney information regarding your care and payment for your care in the event a legal situation occurs.

C. Uses and disclosures with authorization

For **all** other purposes which do not fall under a category listed under section II (subsections A and B), we will obtain your written authorization to use or disclose your protected health information. Your authorization can be revoked at any time except to the extent that we have relied on the authorization.

III. PATIENT PRIVACY RIGHTS

A. Further restriction on use or disclosure

You have a right to request that we further restrict use and disclosure of your protected health information to carry out treatment, payment, or health care operations, to someone who is involved in your care or the payment for your care, or for notification purposes. We are not required to agree to a request for a further restriction.

To request a further restriction, you must submit a written request to our privacy officer. The request must tell us: (a) what information you want restricted; (b) how you want the information restricted; and (c) to whom you want the restriction to apply.

B. Confidential communication

You have a right to request that we communicate your protected health information to you by a certain means or at a certain location. For example, you might request that we only contact you by mail or at work. We are not required to agree to requests for confidential communications that are unreasonable.

To make a request for confidential communications, you must submit a written request to our privacy officer. The request must tell us how or where you want to be contacted. In addition, if another individual or entity is responsible for payment, the request must explain how payment will be handled.

C. Accounting of disclosures

You have a right to obtain, upon request, an "accounting" of certain disclosures of your protected health information by us (or a business associate for us). This right is limited to disclosures within six years of the request and other limitations. Also in limited circumstances we may charge you for providing the accounting. To request an accounting, you must submit a written request to our privacy officer. The request should designate the applicable time period.

D. Inspection and copying

You have a right to inspect and obtain a copy of your protected health information that we maintain in a designated records set. This right is subject to limitations and we may impose a charge for the labor and supplies involved in providing copies.

To exercise your right of access, you must submit a written request to our privacy officer. The request must: (a) describe the health information to which access is requested, (b) state how you want to access the information, such as inspection, pick-up of copy, mailing of copy, (c) specify any requested form or format, such as paper copy or an electronic means, and (d) include the mailing address, if applicable.

E. Right to amendment

You have a right to request that we amend protected health information that we maintain about you in a designated records set if the information is incorrect or incomplete. This right is subject to limitations. To request an amendment, you must submit a written request to our privacy officer. The request must specify each change that you want and provide a reason to support each requested change.

F. Paper copy of privacy notice

You have a right to receive, upon request, a paper copy of our Notice of Privacy Practices. To obtain a paper copy, contact our privacy officer.

IV. CHANGES TO THIS NOTICE

We reserve the right to change this notice at any time. We further reserve the right to make any change effective for all protected health information that we maintain at the time of the change - including information that we created or received prior to the effective date of the change.

We will post a copy of our current notice in the waiting room for the Center. At any time, patients may review the current notice by contacting our privacy officer.

V. COMPLAINTS

If you believe that we have violated your privacy rights, you may submit a complaint to the Center or the Secretary of Health and Human Services. To file a complaint with the Center, submit the complaint in writing to our privacy officer. We will not retaliate against you for filing a complaint.

VI. LEGAL EFFECT OF THIS NOTICE

This notice is not intended to create contractual or other rights independent of those created in the federal privacy rule.

Acknowledgement of Receipt of Notice

ACKNOWLEDGEMENT OF RECEIPT OF NOTICE AND
CONSENT TO USE AND DISCLOSE HEALTH INFORMATION

Read before signing the Acknowledgment and Consent

This acknowledgment of notice and consent authorizes State Hill SurgiCenter to use and disclose health information about you for treatment, payment, and health care operations purposes.

Notice of Privacy Practices. State Hill SurgiCenter has a Notice of Privacy Practices, which describes how we may use and disclose your protected health information and how you can access your protected health information and exercise other rights concerning your protected health information. You may review our current notice prior to signing this acknowledgment and consent.

Amendments. We reserve the right to change our Notice of Privacy Practices and to make the terms of any change effective for all protected health information that we maintain, including information created or obtained prior to the date of the effective date of the change. You may obtain a revised notice by submitting a written request to our Privacy Officer.

How to contact our Privacy Officer:

Mail: State Hill SurgiCenter
Attention: Privacy Officer
2630 Westview Drive
Wyomissing, PA 19610
Telephone: 610-898-1515 Facsimile: 610-898-1525

Acknowledgment and Consent

I have received the Notice of Privacy Practices for State Hill SurgiCenter. State Hill SurgiCenter is authorized to use and disclose health information about _____ (patient name) for treatment, payment, and healthcare operations purposes consistent with its Notice of Privacy Practices.

_____ _____
Signature of patient Date
(or patient's personal representative)

Personal representative information (if applicable):

_____
Name of personal representative

_____
Relationship to patient (or other authority)

STATE HILL SURGICENTER

ACKNOWLEDGEMENT OF RECEIPT OF PRIVACY NOTICE AND PATIENT RIGHTS

I acknowledge that I have received the Notice of Privacy Practices for State Hill SurgiCenter.

_____ _____

Signature of Patient
(or patient's personal representative

Date of receipt

I acknowledge that I have received a copy of Patient Rights for State Hill SurgiCenter

_____ _____

Signature of Patient
(or patient's personal representative

Date of receipt

Personal representative information (if applicable):

_____

Name of personal representative

_____

Relationship to patient (or other authority)

Good Faith Efforts to Obtain Acknowledgement

GOOD FAITH EFFORTS TO OBTAIN
ACKNOWLEDGMENT OF RECEIPT OF NOTICE

For facility use only when efforts to obtain acknowledgment of receipt of notice are unsuccessful.

_____
Name of patient

Personal representative information (if applicable):

_____
Name of personal representative

_____
Relationship to patient (or other authority)

I provided the above named ☐ patient ☐ personal representative with the Notice of Privacy Practices for State Hill SurgiCenter.

Describe how notice was provided:
☐ Offered copy and individual refused to accept delivery
☐ Offered copy and individual accepted delivery
☐ Other _____

_____

_____

_____

Describe efforts to obtain signature on acknowledgment of notice form:
☐ Patient/personal representative was asked to sign form and refused.
☐ Other _____

_____

_____

_____

_____ _____
Signature Date

_____
Print name

Authorization Form

AUTHORIZATION TO USE AND/OR DISCLOSE HEALTH INFORMATION

Read entire document before signing

This authorization gives State Hill SurgiCenter permission to use and/or disclose health information about you.

Right not to sign. You may refuse to sign this authorization. Refusal to sign this authorization will not affect your ability to obtain treatment by State Hill SurgiCenter except in the case of health care that is solely for the purpose of creating health care information for disclosure to a third party.

Right to revoke. You may revoke this authorization at any time except to the extent that we have relied on the authorization. To revoke this authorization, you must submit a written revocation to our privacy officer at the following address:

State Hill SurgiCenter
Attention: Privacy Officer
Address: 2630 Westview Drive
Wyomissing, PA 19610

Re-disclosure. Health information disclosed pursuant to this authorization may be subject to re-disclosure because it is no longer protected by the federal privacy rule or another privacy law.

Authorized uses and disclosures

Print or type all information except signature.

1. Patient name: _____

2. Covered health information – Describe the covered PHI in a specific and meaningful fashion:

_____

_____

_____

_____

3. Identity of user/discloser – Provide the name or other specific identification of the person(s) or class of persons authorized to use and/or disclose the covered information:

_____

_____

_____

_____

4. Authorized action(s): ☐ uses ☐ disclosures (check one or both boxes, as applicable).

5. Identity of recipient – Provide the name or other specific identification of the person(s) or class of persons to whom the covered entity may disclose the covered information (not necessary if only uses are authorized):

6. Each purpose of the authorized uses and disclosures ("At request of individual" is sufficient for uses and disclosures initiated by the patient):

7. Expiration of authorization – Provide a date or event that relates to the patient or the purpose of the use and/or disclosure:

I have read and understand this authorization, and authorize use and disclosure of health information about the named patient as described in this authorization.

Signature of patient (or personal representative) Date

Personal Representative Information (if applicable):

Name of personal representative

Relationship to patient (or other authority)

Re-Disclosure Notices

Re-Disclosure Notices

State Hill SurgiCenter will restrict uses and disclosures for PHI containing information regarding substance abuse, HIV/AIDS, and psychotherapy notes. There are more stringent laws related to this type of information.

PHI containing information related to substance abuse and HIV/AIDS shall only be disclosed to third parties upon written authorization by the patient *unless* the disclosure is to another health care provider for treatment purposes.

PHI containing psychotherapy notes can only be disclosed to third parties upon written authorization by the patient, except where required by law, to protect the individual or a third party from harm, or to defend the provider against a legal proceeding brought by the patient. Psychotherapy notes are defined as notes recorded by a mental health professional that concern the conversation during a counseling session and are separated from the rest of the medical record.

The following language will be included with any disclosure of PHI containing information regarding substance abuse, HIV/AIDS, or psychotherapy notes.

HIV RELATED INFORMATION—NOTICE

This information has been disclosed to you from records protected by Pennsylvania law. Pennsylvania law prohibits you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or is authorized by the Confidentiality of HIV-Related Information Act. A general authorization for the release of medical or other information is not sufficient for this purpose.

MENTAL HEALTH CARE – RE-DISCLOSURE NOTICE

This information has been disclosed to you from records whose confidentiality is protected by State statute. State regulations limit your right to make any further disclosure of this information without prior written consent of the person to whom it pertains.

DRUG AND ALCOHOL ABUSE TREATMENT – RE-DISCLOSURE NOTICE

This information has been disclosed to you from records protected by Federal confidentiality rules (42 CFR part 2). The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 C.F.R. Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient.

Accounting for Disclosures

ACCOUNTING OF DISCLOSURES

Patient Name: _____ Social Security # _____

Date	Information disclosed to whom	Disclosed information	Purpose of disclosure

Business Associate Agreement

BUSINESS ASSOCIATE AGREEMENT

The parties to this agreement are State Hill SurgiCenter ("Covered Entity"), an ambulatory surgery facility located at 2630 Westview Drive, Wyomissing, PA and _____ ("Business Associate"), a _____, with its principal office at _____ (collectively, the "Parties").

Covered Entity is subject to the following rules promulgated by the Department of Health and Human Services ('DHHS") under the Health Insurance Portability and Accountability Act ("HIPAA"):

- Privacy Rule (a/k/a Standards for Privacy of Individually-Identifiable Health Information) – This rule is published at 45 C.F.R. Part 164. It establishes standards for the privacy of personal health information. Covered Entity is required under the rule to obtain privacy assurances from certain entities to which it discloses health information protected by the rule ("PHI") and/or which it allows to create or receive PHI on its behalf.

- Transactions and Code Sets Rule – This rule is published at 45 C.F.R. Part 162. It establishes standards for electronic submission of claims and other health care transactions ("Transactions"). Covered Entity is required under the rule to require certain entities which conduct Transactions in whole or part on its behalf to comply with the rule with respect to such Transactions and to require their agents and subcontractors to comply with the rule with respect to such Transactions.

The Parties agree to be legally bound to the terms and conditions set forth in this Agreement.

I. Definitions.

"Individual" shall have the same meaning as the term "individual" in 45 C.F.R. §164.501 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

"Other state and federal privacy laws" include, but are not limited to professional licensing regulations for physicians (49 Pa. Code §16.61, §25.213), the Confidentiality of HIV-Related Information Act (35 P.S. §§7601-7612), the Mental Health Procedures Act and regulations (50 P.S. §7111; 55 Pa. Code §5100.31-5100.39), and the federal protections for drug and alcohol abuse treatment records (42 U.S.C. 290dd-2; 42 C.F.R. §§2.1-2.67).

"Privacy Rule" shall mean the Standards for Privacy of Individually-Identifiable Health Information promulgated by the Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act at 45 C.F.R. Part 164.

"PHI" shall have the same meaning as the term "PHI" in 45 C.F.R. §164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

"Required By Law" shall have the same meaning as the term "required by law" in 45 C.F.R. § 164.501.

"Secretary" shall mean the Secretary of the Department of Health and Human Services or his or her designee.

"Transaction" means a transaction subject to the Transactions and Code Set Rule.

"Transactions and Code Set Rule" shall mean the Transactions and Code Set rule promulgated by the Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act at 45 C.F.R. Part 162.

II. Permitted Uses and Disclosures by Business Associate.

A. General uses and disclosures. Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity, provided that such use or disclosure would not violate the Privacy Rule.

B. Specific uses and disclosures. Except as otherwise limited in this Agreement, Business Associate may use PHI in accordance with 45 C.F.R. §164.504(e)(4)(I) for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

Except as otherwise limited in this Agreement, Business Associate may disclose PHI to third parties in accordance with 45 C.F.R. § 164.504(e)(4)(ii) for the proper management and administration of the Business Associate, provided that (I) the disclosures are Required By Law, or (ii) Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached

Except as otherwise limited in this Agreement, Business Associate may use PHI to provide Data Aggregation services to Covered Entity as permitted by 42 C.F.R. §164.504(e)(2)(I)(B).

III. Obligations and Activities of Business Associate.

A. Business Associate agrees to not use or further disclose PHI other than as permitted or required by the Agreement or as required by law.

B. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by this Agreement.

C. Business Associate agrees to report to Covered Entity any use or disclosure of the PHI not provided for by this Agreement.

D. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by Business Associate on behalf of Covered Entity agrees to the same restrictions and conditions that apply through this Agreement with respect to such information.

E. Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner designated by Covered Entity, to PHI in a Designated

Record Set (as defined by Covered Entity), to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 C.F.R. §164.524.

F. Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 C.F.R. §164.526 at the request of Covered Entity or an Individual, and in the time and manner designated by Covered Entity.

G. Business Associate agrees to make internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity available to the Covered Entity, or at the request of the Covered Entity to the Secretary, in a time and manner designated by the Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

H. Business Associate agrees to make internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity available to the Covered Entity, in a time and manner designated by the Covered Entity, for purposes of Covered Entity determining Business Associate's compliance with this Agreement.

I. Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528.

J. Business Associate agrees to provide to Covered Entity or an Individual, in time and manner designated by Covered Entity, to PHI in a Designated Record Set, to Covered Entity, or as directed by Covered Entity, to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. §164.528.

K. Notwithstanding any other provision in this Agreement, Business Associate shall comply with other state and federal privacy laws (except to the extent that they are pre-empted by the Privacy Rule) and shall not engage in any activity that would result in Covered Entity being in violation of any other state or federal privacy law.

L. If Business Associate conducts a Transaction in whole or part for or on behalf of Covered Entity, Business Associate shall comply with all applicable requirements of the Transactions and Code Sets Rule and require any agent or subcontractor to comply with all applicable requirements of the Transactions and Code Set Rule.

IV. Obligations of Covered Entity

A. Covered Entity shall provide Business Associate with the notice of privacy practices that Covered Entity produces in accordance with 45 C.F.R. § 164.520, as well as any changes to such notice.

B. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by an Individual to use or disclose PHI, if such changes affect Business Associate's permitted or required uses and disclosures.

C. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. §164.522, if the restriction affects Business Associate's permitted or required uses and disclosures.

D. Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by Covered Entity, except for data aggregation or management and administrative activities of the Business Associate that are authorized in this Agreement.

V. Term and Termination

A. Term. The Term of this Agreement shall be effective as of _____, and shall terminate when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section V.

B. Termination for Cause.

C. Material Breach. In the event that Covered Entity determines that Business Associate has materially breached this Agreement, Covered Entity may either (I) immediately terminate this Agreement and any other related agreements or (ii) provide Business Associate with an opportunity to cure the breach in accordance with Section V.B.2. In the event of a termination pursuant to this section, the provisions of Section V.C shall apply.

1. Opportunity to cure option. Covered Entity may elect to notify Business Associate of a material breach and provide Business Associate with the opportunity to cure the breach upon mutually satisfactory terms. Provided however, in the event that the Parties do not agree to mutually satisfactory terms within 15 days, Business Associate shall cure the breach to the satisfaction of the Covered Entity within 15 days. Business Associate's failure to cure a breach as set forth in this subsection is grounds for the immediate termination of this Agreement, and any other related agreements.

D. Effect of Termination.

1. **Return or Destruction of PHI.** Except as provided in Section V.C.2, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI.

2. Return or Destruction Infeasible. In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of PHI is infeasible, Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

VI. Miscellaneous.

A. Regulatory References. A reference in this Agreement to a section in the Privacy Rule means the section as in effect or as amended, and for which compliance is required.

B. Interpretation. Any ambiguity in this Agreement shall be resolved in a favor of a meaning that permits Covered Entity to comply with the Privacy Rule.

C. Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act, Public Law 104-191.

D. Survival. The respective rights and obligations of Business Associate under Section V.C of this Agreement shall survive the termination of this Agreement.

STATE HILL SURGICENTER	**BUSINESS ASSOCIATE**
By: _____	By: _____
Print Name: _____	Print Name: _____
Print Title: _____	Print Title: _____
Date: _____	Date: _____

Confidentiality Agreement

HIPAA CONFIDENTIALITY AGREEMENT

This HIPAA Confidentiality Agreement ("Agreement") between State Hill SurgiCenter, and _____, is effective as of the date the last party signs this Agreement.

RECITALS

A. State Hill SurgiCenter utilizes certain information ("Information") which may be inadvertently seen by _____ in the course of services performed by _____ some of which may constitute Protected Health Information ("PHI").

B. State Hill SurgiCenter intends to protect the privacy and provide for the security of PHI seen by _____ pursuant to the Agreement in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA") and regulations promulgated there under by the U.S. Department of Health and Human Services (the "HIPAA Regulations") and other applicable laws.

C. The purpose of this Agreement is to satisfy certain standards and requirements of HIPAA and the HIPAA Regulations, including, but not limited to, Title 45, Section 164.504(e) of the Code of Federal Regulations ("CFR"), as the same may be amended from time to time.

In consideration of the mutual promises below and the continuation of the Agreement, the parties agree as follows:

1. Definitions.

   a. "Protected Health Information" or "PHI" means any information, whether oral or recorded in any form or medium: (I) that relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual, and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under HIPAA and the HIPAA Regulations, including, but not limited to 45 CFR Section 164.501.

2. Obligations of _____.

   a. Nondisclosure. _____ shall not use or further disclose State Hill SurgiCenter PHI other than as permitted or required by this Agreement or as required by law.

   b. Safeguards. _____ shall use appropriate safeguards to prevent uses or disclosures of State Hill SurgiCenter's PHI.

c. Reporting of Disclosures. _____ shall report to State Hill SurgiCenter any disclosure of State Hill SurgiCenter's PHI of which _____ becomes aware.

d. Agents. _____ shall ensure that any agents, including subcontractors agree to the same restrictions and conditions that apply to _____ with respect to such PHI.

3. Termination. Material Breach. A violation of a material term of the Agreement by _____as determined by State Hill SurgiCenter shall provide grounds for immediate termination of the Agreement by State Hill SurgiCenter.

4. Indemnification. _____ will indemnify, hold harmless and defend State Hill SurgiCenter from and against any and all claims, losses, liabilities, costs and other expenses incurred as a result of, or arising directly or indirectly out of or in connection with any breach of this Agreement.

5. Interpretation. This Agreement shall be interpreted as broadly as necessary to implement and comply with HIPAA, HIPAA Regulations and applicable state laws.

The parties agree that any ambiguity in this Agreement shall be resolved in favor of a meaning that complies and is consistent with HIPAA and the HIPAA Regulations.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement.

STATE HILL SURGICENTER **ORGANIZATION**

By:_____ _____

Print Name: _____ _____

Title _____ _____

Date:_____ _____

ATTACHMENT A

JOB DESCRIPTION
HIPAA PRIVACY and SECURITY OFFICER

Reports to: The privacy and security officer reports to the governing body of the State Hill SurgiCenter.

Summary: The HIPAA privacy officer is responsible for overseeing the development and implementation of State Hill SurgiCenter's privacy policies and practices. The privacy officer is responsible for coordinating all of the Center's activities that have privacy implications. In addition, the privacy officer is responsible for monitoring the Center's services and systems to ensure it has meaningful practices with regard to privacy. The privacy officer is also responsible for advocating and protecting the privacy of the Center's patients.

Essential duties and responsibilities:

- Reports to the governing body on current and emerging federal and state legislation and regulations impacting privacy and security. Makes recommendations as to how the Center should comply with these regulations.
- Keeps the governing body apprised as to the status of the Center's implementation of privacy and security regulations.
- Coordinates the activities of the implementation team.
- Develops and oversees the Center's implementation plan.
- Documents the Center's privacy and security policies and procedures.
- Monitors compliance with the Center's privacy and security policies. Responsible for documenting and responding to any problems that occur.
- Conducts privacy risk assessments and internal privacy and security audits for the Center.
- Monitors internal controls to ensure that information access levels and security clearances are maintained.
- Prepares the Center's disaster recovery and business continuity plans for information systems

- Develops an employee training program regarding privacy and security requirements. Ensures that all new employees are trained within 30 days of their employment with the Center.

- Ensures that the Center appropriately protects and maintains patient information.

- Manages patient privacy disputes and requests for changes to their medical records.

- Educates the public with regards to the Center's efforts to ensure the privacy of its patients.

- Attends update sessions and/or training programs provided by outside organizations to keep abreast of new developments.

- Updates employees on new developments in privacy and security.

Qualifications:

Must have good communication skills and leadership ability.

Must possess high level of integrity and trust.

Must have conflict resolution skills.

Must be able to manage projects and have good organizational skills.

_____ _____

Signature Date

ATTACHMENT B

HIPAA Training Record

Training Session Date _____

Description of training session (attach any training materials used):

_____
_____
_____
_____
_____
_____

Please sign below to indicate that you have attended this training session. By signing this form you agree to the following statement:

I received and understand the training that was presented today.
I understand that it is my responsibility to apply what I learned today to my daily job functions where applicable.

_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

This training record must be kept on file until _____ (six years from training session date).