



**TORRANCE SURGERY CENTER**  
**HIPAA PRIVACY REGULATIONS COMPLIANCE POLICY**

Torrance Surgery Center (the "Company") has established this compliance policy to ensure that its ambulatory surgery centers (the "ASCs") comply with the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Regulations") promulgated under the Health Insurance Portability and Accounting Act of 1996 ("HIPAA"). Compliance with the Privacy Regulations is important because the failure to comply is a criminal violation and can lead to serious financial and/or criminal liability for individuals and organizations.

This compliance policy is not intended to be a comprehensive explanation of the Privacy Regulations, nor will it provide answers to every possible issue that may arise under the Privacy Regulations. Rather, it is intended to provide guidelines with respect to the steps that the ASCs must take in order to achieve compliance with the Privacy Regulations and to sensitize the ASCs to potential problems that may arise under the Privacy Regulations. The Company expects full compliance with the guidelines set forth in this policy statement, and encourages the ASCs to seek any further necessary information or clarification prior to engaging in any potentially sensitive actions or activities.

This compliance policy is divided into two main sections: (1) an overview of the Privacy Regulations; and (2) specific compliance guidelines. This policy requires the ASCs to:

1. Appoint a Privacy Official;
2. Inform Patients of the ASC's Privacy Policies and Procedures by disseminating handouts and posting a disclosure notice;
3. Use a patient consent and authorization;
4. Use a Business Associates agreement;
5. Clarify discipline for employees and vendors who violate the Privacy Rules and Privacy Policies and Procedures;
6. Update the Privacy Policies and Procedures as needed;
7. Hold all-employee educational meetings;
8. Discuss adoption of the Privacy Policies and Procedures at a Board Meeting; and
9. Develop safe guards to protect and de-identify Protected Health Information (as defined in the regulations).

\\3130600003\CII\2601 14DOC



## **SECTION 1: OVERVIEW OF THE PRIVACY REGULATIONS**

Congress enacted 1-1 I PAA in 1996, in part, to provide for the regulation of the privacy of health information and the simplification of administration of health insurance. The Secretary of Health and Human Services published the Privacy Regulations pursuant to HIPAA on December 28, 2000, 65 Fed. Reg. 82462, 45 CFR Parts 160 and 164. The Privacy Regulations set forth certain protections that health plans, health care clearinghouses, and health care providers ("Covered Entities") must implement in their use and handling of all medical records and other individually identifiable health information, which is in any form, whether electronic, on paper or oral, and which is held or transmitted by a Covered Entity ("Protected Health Information" or "PHI"). The Privacy Regulations' protections are designed to guard against the misuse or unauthorized disclosure of patients' health records and medical information. The Privacy Regulations became effective on April 14, 2001 and generally provide Covered Entities, such as the ASCs, two years within which to achieve compliance from the effective date. Penalties for non-compliance range from a fine of \$100 per person, per incident for unintentional disclosures (which can total up to \$25,000 per person per year) up to a fine of \$250,000 plus 10 years in jail for selling medical information.

## **SECTION 2: COMPLIANCE GUIDELINES**

### **A. Privacy Official**

Each of the ASCs' Board of Managers shall appoint a Privacy Official. The Privacy Official shall report to the Medical Advisory Committee and oversee the compliance plan. The Privacy Official shall be responsible for:

1. developing and implementing compliance policies and procedures of the ASC;
2. overseeing and monitoring the ASC's compliance activities;
3. maintaining compliance;
4. ensuring that all policies are kept current and are followed by all employees;
5. distributing policies that are readily understandable to all employees who handle or use PHI;
6. serving as the ASC's contact person to answer questions and receive complaints regarding the ASC's PHI practices and compliance with the Privacy Regulations; and
7. performing other functions as specified throughout this policy statement.



#### B. Privacy Policies and Procedures

The Privacy Official shall develop and implement written compliance policies and procedures (the "Privacy Policies and Procedures") that (1) address administrative, technical and physical safeguards to protect the privacy of PHI against any reasonably anticipated threat to the privacy of PHI or any unauthorized disclosure of the information, (2) limit the access, use, disclosure and request of PHI to the minimum extent necessary to accomplish the intended purpose, and (3) provide for a process by which individuals may file complaints regarding the Privacy Policies and Procedures or compliance therewith. The written policies and procedures shall be distributed to all employees and members of each of the ASCs.

#### C. Educational and Training Programs

Prior to the April 14, 2003 compliance date, all employees of each of the ASCs shall attend training and educational programs regarding the Privacy Regulations and the Privacy Policies and Procedures. Thereafter, the employees shall attend training and educational programs periodically for updates on new developments with respect to the Privacy Regulations or the Privacy Policies and Procedures. These programs shall be designed to:

1. teach employees what practices and procedures are required under the Privacy Regulations and what procedures should be used under the compliance policy;
2. emphasize the ASC's commitment to compliance with the Privacy Regulations; and
3. reinforce to employees that strict compliance with the Privacy Regulations and the Privacy Policies and Procedures is a condition of employment.

New employees of the ASCs shall be provided training with respect to the Privacy Regulations and the Privacy Policies and Procedures within reasonable time after hire.

#### D. Employee/Vendor Sanctions

Strict compliance with the Privacy Regulations and the Privacy Policies and Procedures is a condition of an employee's employment with the ASCs or of a vendor's business with the ASCs. Accordingly, the ASCs shall sanction employees, vendors and agents who violate the Privacy Policies and Procedures or the Privacy Regulations.

#### E. Written Consent

Each of the ASCs shall use a written consent and disclosure (an example is attached hereto as Exhibit A), which, when signed, shall allow the ASC to use and disclose a patient's PHI for treatment, payment, and health care operations as permitted under the Privacy Regulations. The ASC shall present the consent to each of its patients, accompanied by a notice (as described in Section H) that contains a detailed discussion of the ASC's health information practices. The ASC shall obtain the written consent of each of its patients prior to using or disclosing PHI to carry out treatment, payment, or health care operations. The written consent shall:



1. be in plain language
2. inform the patient that the ASC may use and disclose the patient's PHI for purposes of carrying out health care operations, treatment and payment;
3. refer the patient to the ASC's notice for further information about the ASC's privacy practices;
4. inform the patient that he or she has the right to request restrictions on the ASC's uses and disclosures of PHI;
5. state that the ASC is not required to agree to the patient's request, but that if the ASC does agree to the request, the restriction is binding on the ASC;
6. indicate that the patient has the right to revoke the consent in writing, except to the extent that the ASC has taken action in reliance on the consent; and
7. include the patient's signature and the date of signature.  
The ASCs shall encourage their patients to discuss how the PHI shall be used and disclosed within the health care system.

#### F. Use of PHI without Written Consent

Each of the ASCs shall only use or disclose PHI to carry out treatment, payment, or health care operations without the patient's consent if:

1. the ASC created or received the PHI in the course of providing health care to a patient who is an inmate; or
2. in emergency treatment situations, if the ASC attempts to obtain such consent as soon as reasonably practicable after the delivery of such treatment; or
3. if the ASC is required by law to treat the individual, and the ASC attempts to obtain such consent but is unable to obtain such consent; or
4. if the ASC attempts to obtain such consent from the patient but is unable to do so due to substantial barriers to communicating with the patient, and the ASC determines, in the exercise of professional judgment, that the patient's consent to receive treatment is clearly inferred from the circumstances.

#### G. Authorization

Each of the ASCs shall use an authorization (an example is attached hereto as Exhibit B) that allows the ASC or a third party to use and disclose PHI for purposes other than treatment, payment and health care operations. The authorization shall be written in plain language and in specific terms. The authorization shall include:

1. a description of the information to be used or disclosed;



2. the name of the person or class of persons who is authorized to use or disclose the PHI;
3. the name of the person who is authorized to receive the PHI;
4. an expiration date or an event upon which expiration of the authorization occurs;
5. a notice of the patient's right to revoke the authorization in writing and instructions on how the patient may revoke the authorization;
6. an explanation that the information, if used or disclosed, may be subject to redisclosure by the recipient and is no longer protected by the Privacy Regulations; and
7. the individual's signature and date of signature.

#### H. Notice

Each of the ASCs shall make available to its patients a written notice (an example is attached hereto as Exhibit C), detailing the ASC's health information practices. The notice shall contain a header that reads: **"THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."**

The notice shall contain the following information:

1. a description of all of the uses and disclosures that the ASC is permitted or required to make under the Privacy Regulations without the patient's written consent or authorization;
2. a description, including at least one example, of the types of uses and disclosures that the ASC is permitted to make under the Privacy Regulations with the patient's consent for the purposes of treatment, payment and health care operation;
3. a statement that all uses and disclosures not describe pursuant to sections (1) and (2) above shall be made only with the patient's authorization and that the patient has the right to revoke such authorization;
4. a statement informing patients that they have the right to see, make copies of, and request amendments to their own records and to request restrictions on certain uses and disclosures;
5. a statement informing patients they shall have access to a history of all non-routine disclosures of their PHI made by the ASC;
6. a statement that the ASC is required by law to protect patients' PHI, abide by the terms of the Notice, and inform patients whenever the ASC revises the Notice; and
7. a description of how patients can file a complaint against the ASC for violations of the Notice or Privacy Regulations, the name of a contact person at the ASC, and the effective date of the Notice.



#### I. When and How to Provide Notice

The ASCs shall:

1. post the notice conspicuously in their waiting areas;
2. provide a copy to each patient, new or existing, as of the date of the first service delivery after the compliance date; and
3. provide additional copies to patients upon request.

#### J. Business Associates

Each of the ASCs shall enter into a contract (an example is attached hereto as Exhibit D) with all business associates who may come into contact with PHI, such as data processing, administrative services or billing services ("Business Associates"). Business Associates include any person or corporation that uses PHI *on behalf of* the ASC. For example, when an ASC discloses PHI to health plans for payment purposes, no business associate relationship is established. While the ASC may have an agreement to accept discounted fees as reimbursement for services provided to health plan members, neither entity is acting on behalf of or providing a service to the other.

An ASC may disclose PHI to a Business Associate and may allow a Business Associate to create or receive PHI on its behalf, if the ASC obtains satisfactory assurance, in the form of a written contract, that the Business Associate will appropriately safeguard the information. The Business Associate contract must contain provisions whereby the Business Associate agrees to:

1. abide by the ASC's Privacy Policies and Procedures;
2. not use or further disclose the PHI except as permitted;
3. implement and use appropriate safeguards to prevent the unauthorized use and disclosure of PHI and to comply with the law;
4. make available P1-IL upon patient request and for amendment purposes;
5. report to the ASC any use or disclosure not provided for in its contract with the ASC;
6. make available the information required to provide an accounting of disclosures;
7. make its books and records relating to PHI received from the ASC available to the Secretary of Health and Human Services for purposes of determining the ASC's compliance with the Privacy Regulations; and
8. at termination of the contract with the ASC, if feasible, return or destroy all PHI received from, or created or received by the Business Associate on behalf of, the ASC.

#### K. De-Identify Information



The ASCs shall adopt a policy to encourage the deletion of all identifying information from PHI before transmission in order to allow the ASCs to use and disclose the de-identified information without obtaining consent from their patients.

Because properly de-identified information is not subject to the requirements of the Privacy Regulations unless it is re-identified, the ASCs may use PHI to create information that is not individually identifiable health information or disclose PHI to a Business Associate for such purposes, whether or not the de-identified information is to be used by the ASCs.

#### L. Uses and Disclosures Required by Law

The ASCs may use or disclose PHI in order to comply with laws requiring the use or disclosure of PHI, provided the use or disclosure meets and is limited to the relevant requirements of such other laws. "Required by law" means a mandate contained in a law that compels an ASC to make a use or disclosure of PHI and that is enforceable in a court of law. Examples include court-ordered warrants, and subpoenas issued by a court. It does not include contracts between private parties or similar voluntary arrangements. If the information is "required by law," it is not subject to the consent requirement. The ASCs need not make a use or disclosure required by the legal demands or by any other law or legal process, and may challenge the validity of such laws and processes.

#### M. Written Records

The Privacy Official shall maintain a written record of all actions, activities, designations, consents and authorizations required under or taken in accordance with this compliance policy, the Privacy Policies and Procedures or the Privacy Regulations. Such records shall be maintained for a period of six years from the date of creation or the date when such records were last in effect, whichever is later.