STAR Spine & Sport
HIPAA Privacy Rule Overview

Implementation date: 02/01/2014 Revision Date: 02/01/2014

Approvals: Lisa M. Schumacher
Title Practice Manager

I. POLICY

It is the policy of Star Spine & Sport (The Practice) to protect and maintain the privacy of the health information of each patient of the Practice in accordance with the requirements of state and federal law, including the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

II. SCOPE

The purpose of this policy is give general guidance as to the requirements of HIPAA as they relate to the privacy of patient health information.

III. DEFINITIONS

Below are definitions for some of the key terms found in HIPAA and used throughout this Policy and in other privacy-related policies of [the Practice].

A. ***Covered Entity*** means a health plan, a health care clearinghouse, or a health care provider that transmits health information electronically as part of certain transactions, including the transmission of health care claims, receipt of health care payments and remittance advice, verification of enrollment in a health plan or submission of a prior authorization request. If a health care provider conducts any one of these transactions electronically (including by facsimile), it is a Covered Entity.

> *The Practice is a health care provider under HIPAA and, because the Practice transmits health information electronically for one or more of the HIPAA covered transactions, the Practice is a Covered Entity under HIPAA.*

B. ***Business Associate*** means an individual or company that performs an administrative function or activity on behalf of the Practice that involves the use or disclosure of patient health information. For example, a company that performs billing or transcription services for [the Practice] is a business associate of the Practice. The Practice is required to enter into a business associate agreement with each of its Business Associates to ensure that each of them abide by the Privacy Rule requirements to the same extent as the Practice is required to adhere to the Privacy Rule. In fact, the Practice could be held accountable for violations committed by a business associate if: 1) the Practice knew that the Business

Associate was breaching its obligations under the Business Associate Agreement; and 2) the Practice did not take steps to mitigate damages and prevent future violations of the Privacy Rule.

C. ***Protected Health Information*** ("PHI") means health information that: 1) is transmitted, received or maintained in any form or medium (e.g., oral, paper or electronic) by the Practice; 2)

D. identifies a patient; and 3) relates to the past, present or future physical or mental health of the patient or the past, present, or future payment for the provision of health care to the patient. For example, PHI is contained in the following places in the Practice: paper or electronic patient medical charts, the computerized patient insurance files, and patient financial files. The Practice's privacy related policies use the phrase "patient health information;" this phrase means the same as PHI.

E. ***Treatment*** means the provision, coordination, or management of health care and related services. Treatment includes consultation between health care providers or the referral of a patient from one health care provider to another.

F. ***Payment*** means activity to obtain payment for services rendered. For example, submitting a portion of a patient's medical record to a health insurance company in order to obtain payment authorization for a particular procedure would be an activity for the purpose of obtaining payment.

G. ***Health Care Operations*** relates to the Practice's internal administrative processes, including the following activities: 1) quality assessment and improvement; (2) utilization review activities; 3) credentialing employees and the professional review of health care professionals; 4) legal services; 5) accounting and auditing services; 6) business planning and development; 7) actuarial services; and 8) business management and other administrative activities. For example, conducting quarterly audits of physician charts and insurance claims would be an activity that relates to the Practice's health care operations.

IV. GENERAL GUIDANCE REGARDING PRIVACY OF PHI

A. Limiting Use and Disclosure of PHI

1. The Practice and its business associates generally may not use or disclose a patient's PHI unless the use or disclosure fits into one of the following categories:

   a. ***Treatment, Payment or Healthcare Operations ("TPO").*** The Practice must distribute its Notice of Privacy Practices and attempt to obtain a written acknowledgement of receipt from each new and existing patient of the practice. Once a patient has been given the Notice, the Practice may use or disclose the patient's PHI for the treatment of the patient, for obtaining payment for services rendered or for conducting the Practice's health care operations, as those terms are defined in Section III above. Additionally, the Practice may disclose a patient's PHI to: a) another health care provider for the purposes of treating the patient; b) another Covered Entity if the PHI is necessary in order for the entity to obtain payment for services rendered to the patient; or c) any Covered Entity that has a relationship with the patient for purposes of conducting the Covered Entity's health care operations.

   b. ***Patient Authorization***. If a patient's PHI will be used or disclosed for some purpose other than TPO (e.g. disclosed to a life insurance company), the Practice must obtain an

authorization for release of information. For example, the Practice must obtain authorization before using a patient's name and address for marketing purposes. Generally, an authorization is needed to disclose PHI to persons outside the practice.

c. ***Special Circumstances***. The Practice may use or disclose a patient's PHI without obtaining written authorization if it is required by law. Some of the situations include: a) the collection of PHI by public health authorities for public health activities; b) reporting victims of abuse or neglect; or c) receipt of a court order for medical records. If the Practice intends to use or disclose PHI for a purpose other than TPO and the Practice does not have the patient's written authorization, the Practice should consult with legal counsel to determine whether any of the special circumstance exceptions may apply to allow the use and/or disclosure of PHI.

B. Minimum Necessary Standard

1. The Practice must establish procedures and revise job descriptions and policies to reasonably ensure that it limits the use of disclosure of the PHI to the "minimum necessary" to accomplish the purpose of the use or disclosure. For example, the Practice's accountant may need access to a patient financial information in order to balance the Practice's book; however, the accountant should not be granted access to the patient medical information since that PHI is not necessary to accomplish his/her duties. Similarly, the receptionist may need access to a patient's name and phone number to make an appointment reminder call; however, the receptionist should not be granted access to patient health information since that PHI is not necessary to accomplish her duties.

The "minimum necessary" rule does not, however, apply to the following:

a. Disclosures to a health care provider for treatment purposes;
b. Disclosures to the patient who is the subject of the PHI;
c. Uses or disclosures made pursuant to the patient's written authorization;
d) Uses or disclosures made to the Department of Health & Human Services; or
e) Uses or disclosures that are required by law.

C. Patient Rights.

The Privacy Rule establishes six specific patient rights designed to allow patients some degree of control over the confidentiality and privacy of their PHI. The Privacy Rule prohibits the Practice from requiring individuals to waive any of the rights summarized below before providing treatment to the individuals.

1. ***Adequate Notice of Privacy Practices***. The Practice must create a written notice that describes the Practice's policies and procedures for protecting the privacy of PHI. The Notice of Privacy Practices ("NPP") must comply with the specifications of the Privacy Rule by including a description of the Practice's privacy policies and procedures, listing the patient rights, providing the name of a contact person who can answer privacy questions and informing the patient of how to file a complaint regarding the Practice's privacy practices. The Practice must post the NPP in a prominent place for patients to view, provide the NPP to patients no later than the first date of service on or after April 14, 2003, and make copies of the NPP available upon request. For additional information about this patient right, see Policy "Notice of Privacy Practices".

2. ***Access to Health Information***. Patients generally have a right to access, inspect and copy PHI used to make health care or payment decisions about them. The Practice must act upon a patient's request for access within 30 days if the information is located on-site and within 60 days if the information is located off the premises. The one exception to this general right is that a patient does not have the right to access psychotherapy notes.

3. ***Amendment of Health Information***. Patients have the right to request amendment to and correction of their PHI. [The Practice] must respond to the request within 60 days. The Practice may deny the request if the PHI is complete and accurate, but the Practice must inform patients of their options with respect to future disclosures of the disputed information.

4. ***Restriction on Uses and Disclosures***. Patients have the right to request restrictions on the use and disclosure of their PHI. The Practice may accept or reject the request. However, if the Practice grants the request, it must document the restriction and maintain the documentation for a minimum of six years.

5. ***Alternative Methods of Communicating***. Patients have the right to request that the Practice communicate PHI to them by "alternative means" or at "alternative locations." Such requests must be accommodated if reasonable.

Accounting of Disclosures. Patients have the right to receive an accounting of PHI disclosures made by the Practice during the 6 years prior to the date of patient's request for accounting. The accounting of disclosures does not, however, need to include disclosures such as those made prior to the April 14, 2003, disclosures made to carry out treatment, payment or healthcare operations, disclosures made pursuant to the patient's authorization or disclosures made to the patient.

E. Administrative Requirements

1. The Practice must:

a. Have a Privacy Officer. The Practice must designate an individual as the Practice's Privacy Officer. The Privacy Officer is responsible for: i) developing and implementing privacy policies and procedures for the Practice; ii) receiving and responding to privacy-related complaints; and iii) answering questions and providing further information regarding the Notice of Privacy Practices. The privacy officer for [the Practice] is Lisa Schumacher.

b. ***Have Policies and Procedures***. The Practice must develop written policies and procedures that implement the requirements of the Privacy Rule and that are designed to protect the confidentiality and privacy of PHI. For a list of the Practice's written HIPAA Policies, please see Section III.G. of this Policy.

c. ***Conduct Employee Training***. The Practice must train each member of its workforce regarding the Practice's HIPAA privacy policies and procedures. The training may be tailored according to the workforce member's particular job functions. For instance, the receptionist may have different training than nursing staff.

d. ***Have a Complaint System***. The Practice must have a system to allow patients, families and staff to file complaints regarding privacy breaches or the Practice's privacy practices in general. The Practice must investigate the complaint and, if necessary, take actions to correct any deficiencies or problems uncovered by the investigation. The Practice is required by the Privacy Rule to mitigate any harmful effects that occur as a result of a privacy violation by the Practice or its business associates. The Practice cannot intimidate, threaten, discriminate against or generally retaliate against anyone who has filed a complaint or who assists in the investigation.

e. ***Impose Sanctions for Breaches***. The Practice must impose sanctions for staff members who fail to comply with the Practice's HIPAA Policies or the Privacy Rule.

f. ***Retain HIPAA Records***. The Practice must retain its written HIPAA Policies and other documentation created under the Practice's HIPAA Policies for a minimum period of 6 years.

F. Enforcement of the Privacy Rule

In addition to the right to complain to the Practice, patients, families and staff can complain to the federal Office of Civil Rights ("OCR"). OCR will investigate the complaints. OCR can impose a $100 civil fine for each violation, up to a maximum of $25,000 in a calendar year. If an individual or entity knowingly uses or discloses PHI in violation of the Act, OCR cam impose a criminal fine of up to $50,000 or prison for up to 1 year, or both. If the violation is committed under false pretenses, the individual may be subject to a fine of up to $100,000 or prison for up to 5 years, or both. If the violation is committed with intent to sell, transfer or use PHI for commercial advantage, personal gain or malicious harm, the individual may be subject to a fine of up to $250,000 or prison for up to 10 years, or both.

G. HIPAA Policies

- **Authorization For Use and Disclosure**
- **Business Associates**
- **Complaints, Sanctions & Mitigation**
- **Destruction of Health Information**
- **Employee Training**
- **Marketing Practices**
- **Minimum Necessary Standard**
- **Notice of Health Information Practices**
- **Patient Request for Accounting of Health Information Disclosures**
- **Patient Right to Inspect and/or Copy Health Information**
- **Patient Right to Request Alternative Methods of Communication**
- **Patient Right to Request Amendment or Correction of Health Information**
- **Patient Right to Request Restrictions on Uses and Disclosures of Health Information**
- **Privacy Officer Job Description**
- **Record Retention**
- **Technical and Physical Safeguards**