



SOMA Orthopedics Medical Group, Inc. Privacy Policy

Overview: Privacy and Confidentiality

What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that is designed to protect the privacy of patient information, provide for the electronic and physical security of health and patient medical information, and simplify billing and other electronic transactions through the use of standard transactions and code sets. HIPAA applies to all "covered entities" such as hospitals, physicians and other health care providers as well as their employees. Compliance with the HIPAA privacy rules is required by April 14, 2003. Some of the rights provided to patients through the HIPAA privacy rules are:

- The right to receive the "Notices of Privacy Practices" for SOMA.
- The right to request access to their health and research records.
- The right to request an addendum or amendment to the information in their medical record.
- The right to receive an accounting of disclosures of their medical record.
- The right to request restrictions on what protected health information SOMA might release.
- The right to complain if they believe their privacy rights have been violated.

Most of the HIPAA patient rights and protections have existed for years under California state law. New requirements that effect our office include: appointment of a privacy officer; establish administrative, technical and physical safeguards for protected health information (PHI); respond to patient's requests to learn who has accessed their PHI; provide every patient with a "Notice of Privacy Practices" to help explain rights and responsibilities related to their PHI.

What do HIPAA's administrative simplification rules cover?

There are four main provisions in the HIPAA administrative simplification rules:

1. Uniform electronic transaction standards for health care data
2. Privacy and confidentiality provisions for individually-identifiable health care data
3. Security procedures to protect electronically maintained health information
4. Unique health identifiers for providers, employers, plans and individuals to be used in connection with the Uniform Electronic Transaction Standards

When HIPAA rules take effect?

- Privacy Rule.....April 14, 2003
- Uniform Electronic Transaction Standards.....October 16, 2003

Confidential Information

What is considered confidential protected health information (PHI) and what must be protected?

PHI is any information which can be matched with a patient, is created in the process of caring for the patient and is kept, filed, used or shared in an electronic, written or oral manner. Examples include: patient date of birth, address, name, age, medical record number, phone number, diagnoses, prescriptions, lab work, billing data, referrals, authorizations, explanation of benefits. Research records of patient care must also be protected. If health related information is de-identified, it is not PHI and may be shared without restriction. De-identified means the removal of any personally identifying information.

Who can access confidential PHI?

Doctors, Nurse Practitioners and other licensed providers in the office may access the entire medical record, based on their "need to know". **All other employees have access to only the information needed to do their jobs.** The expectation is that employees will apply the "minimum necessary" standard when accessing PHI. Our "Notice of Privacy Practices" describes specifically ways in which we may use PHI without obtaining an authorization from the patient. Basically, we can use the PHI for issues related to TPO:

- **Treatment** of patients, including appointment reminders
- **Payment** of health care bills (claim submission, authorizations, payment posting)
- **Operations** of the practice including teaching, medical staff quality activities, research (when approved by the IRB and with the patient's written informed consent), healthcare communications between a patient and their physician, planning and development.

Written Authorization

Outside of the TPO parameters, written authorization from the patient is required prior to disclosure of PHI. Specific authorization forms will need to be signed by the patient on these occasions. Please read the attached "Notice of Privacy Practices" for the specific list of exceptions to the authorization requirements.

Refusal to Sign Authorization

There may be times when a patient will refuse to sign an Authorization. When this occurs, you should inquire as to why the patient does not want SOMA to use his/her PHI in the manner set forth in the authorization. At no time should you condition treatment or other activity at SOMA on the patient's willingness to sign the authorization.

If patient still refuses to sign authorization and you believe that further discussion would not change the patient's mind, simply note your attempt to have patient sign the authorization form on the form itself (include date, time, and your name), inform provider, and submit the unsigned form to the Privacy Officer.

Speaking Confidentially

Respecting patient privacy and confidentiality is as important as providing any other aspect of care. Staff is sometimes overheard sharing patient information with each other in public areas or private areas that do not provide adequate privacy. Even when we think we are discussing a patient without clear-cut identifiers, we may be breaching the patient's privacy. Please be actively aware of your surroundings when there is a need to discuss anything involving the patient's protected healthcare information.

Incidental Disclosures

It is inevitable that some patient information will be inadvertently disclosed to people not involved in the patient's care. Examining rooms are not completely soundproof. Patients will, on occasion, ask questions about their care while in a public area. A telephone call to a patient to communicate test results might be overheard, or test results might be left where they can be seen by unauthorized persons.

The HIPAA privacy rule recognizes that, on occasion, limited information will be disclosed that out not be disclosed. Such “incidental disclosures” do not violate HIPAA, and we are not required to document them. We should, however, make every effort to minimize these kinds of disclosures.

General Procedures

Check-in/Check-out

To ensure the privacy of our patient’s health information, SOMA prohibits any employee from speaking to patients about their current condition while at the front or back desks, unless there are no other individuals at the front or back desks, except the employee and the patient. If there are other individuals nearby, employees should ask the patient to either step to an area that is empty, ask the patient if you can call them with the information at a later time, or inform patient their question will be answered when the parties can have more privacy.

At no time should any employee leave any forms, medication prescription, specialist referral or other items that contain the patient’s health information on the top of a counter at the front or back desks or anyplace else where they can be viewed by individuals other than the patient.

Consent Form

When a new patient comes into the office for the first time, s/he should be given the SOMA “Notice of Privacy Policy” which outlines our standards on how their medical information is protected, as well as outlines their rights to view and copy their medical information. This Notice is given to the patient in addition to our other new patient forms.

The front desk receptionist should ask the patient to review the Notice and then sign the Consent Form. If a patient has any questions about the Notice or wishes to request restrictions on their health information, the receptionist should call the Privacy Officer if s/he is unable to answer questions. Charts will be marked “Restricted Release of Information” when the patient requests a restriction on his/her PHI.

For an established patient, the receptionist should verify that SOMA has a current consent form signed. If not, follow the procedure above for a new patient.

Calling Patient to Exam Room

When the exam room is ready, the medical assistant or other staff member should go to the waiting area and call the patient’s name. At no time should this individual announce the reason for the patient’s visit, any symptoms the patient may be experiencing, or any tests to be conducted on the patient. The employee is limited to saying the patient’s name and the provider’s name who will see the patient

If the patient asks the employee a question regarding their health status, inform the patient their questions will be answered after they enter the exam room and close the door. Inform patient this is to protect their privacy.

Telephone Conversation

Telephone conversations present SOMA with the most difficulty in protecting our patient’s privacy. One should always be on guard when speaking on the telephone. Never assume you know who the caller is. You must take reasonable steps to verify the caller’s identity. Therefore, before you reveal any personal health information over the telephone, you must take steps to verify the identity of the caller. Questions that can help with this are: Who is your treating physician? What is your date of birth? Who is your insurance carrier? These questions will help identify the caller and help update demographic information. Once you have verified a patient’s identity, you may disclose personal health information to that patient.

Remember, unless we have written authorization from the patient or the disclosure is required by law (see Notice of Privacy Policy), you are not permitted to disclose any personal health information to anyone other than the patient. This includes spouses, children, friends, attorneys, or other representatives of the patient. You may accept information about a patient from spouse, friend, etc., but you cannot reveal any information; ie. If a

spouse calls to make a payment on an account, you can take the information from the spouse, but may not give out anything including the current account balance.

Be careful what messages you leave on answering machines and voice mail. When taking a message over the telephone, you can ask the patient if leaving a message is okay – make sure to note the patient’s response on the message. You can also check the patient demographic form and see if the patient has requested a specific number to be used if leaving a message. If you use speakerphone, be aware of your surroundings and sensitive to the messages being replayed and/or what you are saying.

Faxing PHI

Always check the destination fax number before faxing. Call ahead to ensure that the intended recipient will pick up the fax. Keep a log book of frequently used fax numbers so verification is easy. Return items you receive that were faxed to the wrong location and advise sender of the error. Use cover sheets containing a confidentiality statement such as:

CONFIDENTIALITY NOTICE. This communication and any attachments may contain confidential and privileged information for the use of the designated recipients named above. Distribution, reproduction or any other use of this transmission by any party other than the intended recipient is prohibited.

Email of PHI

Assume normal email systems are not secure unless you have clear information that the system is encrypted or in other ways secure. Do not send confidential information unless you can de-identify it. Warn patients who communicate with you via email that their confidentiality cannot be ensured. Do not send attachments containing protected health information without encryption. Add a confidential message footer to your messages, such as:

CONFIDENTIALITY NOTICE. This email communication and any attachments may contain confidential and privileged information for the use of the designated recipients named above. Distribution, reproduction and any other use of this transmission by any party other than the intended recipient is prohibited.

Computer and Workstation

Never leave an open patient medical record unattended, especially if your workstation is in a highly visible area. Always log-on, and more importantly, log-off any computer terminal that you use to connect to the medical practice’s network. Never leave a computer terminal that is logged on to the network unattended. Other staff or visitors might be able to use the terminal to access patient records. Use your own ID and password. Change password frequently. When you sit at your workstation, only you should be able to see and read the computer monitor. You should therefore adjust the angle of your monitor to prevent other individuals from viewing and reading the information.

Amending a Patient’s Medical Record

Patients who believe information in their medical record is incomplete or incorrect may request an amendment or correction to the information. Follow the steps outlined below when a patient makes such a request.

The patient may approach the author of the entry, point out the error, and ask the author to correct it. Alternatively, the patient can contact the Privacy Officer or other qualified employee to ask for a correction to his/her medical info.

For “simple” corrections, such as name, address, age or other non-medical information, the entry author can correct the entry or add a progress note to clarify content. For more “complicated” corrections, the Privacy Officer should be contacted to assist the patient in completing the health record correction/amendment form.

Upon completion of form, the Privacy Officer will give one copy to the patient, place one copy in the medical record, and give the original, along with the medical record, to the author. If the author chooses to add a

comment to the amendment/correction form, a copy of that will be sent to the patient and the original form with author's signature will replace the copy previously placed in the patient's record.

Copies of the correction/amendment form will be furnished to those individuals or organizations the patient deems necessary and documents on the correction/amendment form. Copies of the correction/amendment form will also be furnished our business associates or others who have the information subject to the amendment and that may have relied or could rely on that information to the detriment of the patient.

When a correction/amendment form is used, there will be an entry at the site of the information that is being corrected or amended indicating, "See correction/amendment". The correction/amendment form will be attached to the incorrect or amended entry.

Whenever a copy of the corrected/amended entry is disclosed, a copy of the correction/amendment form will accompany the disclosed entry.

Requests for Protected Health Information

You may receive a request for a patient's protected healthcare information from a patient (known or unknown) or organization (known or unknown). No matter how insistent the requestor, you cannot disclose any information about the patient without doing the following:

TELEPHONE REQUESTS. If the request was made using the telephone, you should inform the requestor to send you a fax on their official letterhead stating their request (unless we can determine that the requestor is a "known requestor" and we are completely sure that the request is legitimate). Oral requests from unknown individuals over the telephone are not allowed and will not be fulfilled. If the individual making the request does not wish to send a written request, we will be unable to release and information.

You must then determine if the request was made for treatment, payment, or healthcare operation purposes. If request falls outside these areas, the request must include an authorization from the patient to release the information to the requesting party. If you are unsure as to how the information will be used, ask the Privacy Officer to help you.

If the caller is a patient, verify the patient's identity by asking the patient to confirm DOB, address, etc. Let patient give you the information-not the other way around. If a patient spouse or friend calls, verify identity, then make sure there is documentation in chart that authorizes us to release information to this person. If no documentation on file, we cannot release any information. A verbal authorization from the patient is sufficient; when received from patient, make sure it is documented in chart.

Once you have verified the identity of the requestor, received the proper authorization from the patient (if necessary), and entered the request into the patient disclosure log (see appendix forms), you may then send the requested information.

FAX OR MAIL. If the request was submitted via the facsimile machine or via US mail, first determine the origin of the fax or letter. The document should have an official seal, logo, or other identifying mark that clearly establishes the individual or entity requesting the information. It should also include the business name, address, telephone number, and name and title of the individual making the request. The fax or letter must state clearly what information is requested, and for what purpose the individual or entity will use the information. If any of these items are not on the document, or it does not give adequate details, contact the requestor to get more details about the information requested and/or the intended use of that information. For information requested related to a legal proceeding, the fax or letter must be accompanied by a copy of an official judicial subpoena or other court document as required by state law.

Potential Consequences for the Unauthorized Release of PHI

Our patient's privacy is a high priority, and we take unauthorized release of our patients' personal health information seriously. If you observe or have knowledge of any unauthorized release of protected health information from SOMA, you must immediately report this release to the Privacy Officer.

Once the Privacy Officer has knowledge of an alleged unauthorized use or disclosure of PHI, s/he shall immediately begin a thorough investigation of the unauthorized release of PHI. This may be performed through confidential interviews with staff members, inspection of release logs, and other methods the Privacy Officer deems appropriate including asking for assistance from another staff members in conducting the investigation.

Upon concluding the investigation, the Privacy Officer shall implement appropriate changes to policies and /or personnel as s/he deems necessary, and shall do so as expeditiously as possible. The following illustrates how the Privacy Officer may make changes:

“Policy changes: If the Privacy Officer finds the practice policies and/or procedures require adjustments, s/he shall make the necessary modifications to the practice policies by adding addendum(s) to the current policies and shall notify all staff members of the change(s) through inter-office memorandum.

“Personnel changes: If the Privacy Officer finds that one or more staff members either do not understand or refuse to abide by SOMA’s policies and procedures on maintaining the privacy and confidentiality of PHI, it may be necessary for employees to be disciplined by the Privacy Officer for violations of the practice policies. The Privacy Officer shall determine the severity of the punishment based on the severity of the unauthorized release. The following provides a guide as to how the Privacy Officer may discipline the employee:

First Offense: Retraining on the practice’s policies and procedures governing privacy of PHI, and verbal reprimand/counseling, with a note of such filed in employee’s personnel file.

Second Offense: Written reprimand from the Privacy Officer, with a copy to employee and copy filed in employee’s personnel file.

Third Offense: Suspension from duties without pay for a period not to exceed 2 weeks.

Fourth Offense: Termination of the employee.

In all cases, the Privacy Officer shall document in writing the unauthorized use or disclosure of PHI, the perpetrator, and what action(s) were taken as a result of the violation.

Security

HIPAA requires us to secure the electronic and physical access to PHI so that others cannot see or use PHI inappropriately. There are four components to the security rule:

1. Administrative Procedures – policies and procedures to manage and protect data and to manage the personnel in relation to the protection of data.
2. Physical Safeguards – provides for the protection of physical computer systems and related buildings and equipment.
3. Technical Security Services – processes in place to protect information and control individual access to PHI.
4. Technical Security Mechanisms for Networks – processes that guard against unauthorized access to data that is transmitted over a communication network.

“Security policy will be added at a later date.