PRIVACY POLICIES AND PROCEDURES

Practice Name: Coastal Urology of Stuart

Address: 905 SE Monterey Commons
Stuart, Florida 34996

These Privacy Policies and Procedures describe our obligations to protect the privacy of individually identifiable health information that we create, receive or maintain on our patients. The policies and procedures address how we protect their privacy interests and comply with our legal obligations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This written plan addresses our legal responsibilities under HIPAA regulations 45 CFR Parts 160 and 164 (54 Federal Regulation 82462 (12/28/2000) (also referred to as the "Privacy Rules"), as amended (67 Federal Regulations 53182 (8/14/2002), under the HITECH Act breach notification rules as defined in The American Recovery and Reinvestment Act of 2009 (2/17/2009) and state privacy laws that may be more stringent than the federal law. Effective March 26, 2013, HIPAA Regulations 45 CFR Parts 160 and 164 modified Privacy, Security, Enforcement and Breach Notification.

We require all employees, other members of our workforce and Business Associates to follow our Privacy Policies and Procedures. Failure to faithfully follow the rules of our Privacy Plan can result in disciplinary action up to, and including, termination of employment or affiliation with us. All employees and members of our workforce have been trained on our Privacy Plan and are required to sign a Confidentiality Statement.

These written Policies and Procedures address the way HIPAA Privacy Rules apply to this practice and do not cover the entire Rule. In addition to the following Policies and Procedures, we use forms, agreements, contracts, logs, and other documentation to support and comply with our legal obligations. We have elected to use the word "patient" interchangeably with the word "individual", which HIPAA uses in their Privacy Rule. When "patient" is used, it has the same meaning as "individual" and refers to former patients, prospective patients, patients of record and their authorized representatives.

Any questions about our Privacy Plans, the use and/or disclosure of any individually identifiable health information, any of our obligations under the Privacy Rule, or other federal or state laws regarding the privacy rights of our patients, consult our Privacy Officer.

Name of Privacy Officer: Latoya Mills

Phone Number / E-mail / Other Contact Information: 772-288-3301

Effective Date: 12/17/13 *Supersedes previous HIPAA Privacy Policy*

USE AND / OR DISCLOSURE RULE

Our practice will not use and / or disclose protected health information (PHI) unless it is specifically permitted in our written Privacy Plan. Adherence to this concept is one of the key components of our Policies and Procedures. All employees, members of our workforce and our Business Associates understand this rule and will comply with it.

NOTICE OF PRIVACY PRACTICES

Our practice will maintain a **Notice of Privacy Practices** as required by HIPAA Privacy Rules. We will use and disclose protected health information (PHI) only as described in our Notice. Whenever there is a change in the way we use or disclose PHI we will revise the **Notice** to reflect these changes.

Our **Notice of Privacy Practices** will be posted in a prominent location where patients can reasonably see and read it. Our **Notice** is posted, in the following location(s): Waiting room & Website

The **Notice** will be provided to our patients no later than the date of our first service to them after April 14, 2003. It will be available to patients, the patients' representatives and to others. If our Notice is **revised**, patients will be provided with the revised Notice on the date of our first service to them following the revision date. The revised Notice will be posted in a prominent location.

ACKNOWLEDGEMENT OF RECEIPT OF NOTICE

This practice will make a good faith effort to obtain a signed copy of the form **Acknowledgement of Receipt of Notice of Privacy Practices** as required by HIPAA. If, for some reason, we cannot obtain a signed Acknowledgement, we will document the reason or reasons why the acknowledgement wasn't signed. A copy of the **Acknowledgement of Receipt of Notice of Privacy Practices** will be placed in the patient's record.

SIGN-IN SHEETS

This practice has made the following decision regarding the use of sign-in sheets:

- ☐ We will use a sign-in sheet with only the patient's name.
- ☐ The sheet will contain only the patient's name and arrival time (and/or appointment time).
- ☐ The sheets will be changed at least ____ times a day.

- ☐ We will use specialty sign-in forms designed to protect patient privacy; peel off sticker.
- ☑ We will not use a sign-in sheet.

CALLING PATIENTS BY THEIR NAMES IN THE WAITING ROOM

Patients will be called by their name. Because HIPAA allows "incidental oral disclosure" for the purpose of conducting routine business, calling a patient by his/her name is permitted.

Therefore, we will notify patients in the waiting room by addressing them by their name. No individually identifiable information will be communicated. We will use a standard greeting, their name and a statement such as, "The doctor can see you now."

PATIENT SCHEDULES

Patient schedules may contain sensitive information. Realizing this, we have taken steps to protect patient health information from unauthorized disclosure. As a means of protecting patient health information we will take the following steps:

- ☑ We will continue to use printed patient schedules. They will be placed **only** in the following location(s): Nursing schedules & EMR
- ☐ We will not post printed patient schedules.
- ☑ We will use our computer(s) to generate and display patient schedules.
- ☑ We will position the monitors so the screens aren't visible to visitors.
- ☑ We will use screen savers.
- ☑ We require users to log off when the computer isn't in use.

PATIENT CHARTS

The information in patient's charts is privileged information and, with that in mind, this practice will take reasonable measures to protect that information.

- ☑ When charts are pulled for the next day's use, they will be protected by: EMR only
- ☐ Charts will be placed outside treatment areas in such a way that confidential patient information will not be visible.
- ☐ We will place charts inside treatment areas.
- ☑ Patients and visitors will always be escorted in treatment areas.
- ☐ No information will be written on the outside (jacket) of the chart.

- ☐ Charts will not be left open on desks and/or in any areas where unauthorized individuals have access.
- ☐ Information belonging in charts (test results, exam notes, etc.) will be placed in the charts as soon as feasible.
- ☐ Until the staff has the opportunity to file charts, we will keep the charts secure by keeping them Electronic only
- ☐ Charts will be returned to records files as soon as feasible. No charts
- ☐ When the office closes, our records are locked in a records room.
- ☐ When the office closes, our records are secured in locked file cabinets.
- ☐ We have taken other measures to protect health records. They are:

  _____

  _____

  _____

- ☐ We do not use paper charts. We have taken security measures to protect our electronic medical records.

OTHER WAYS WE PROTECT CONFIDENTIALITY OF HEALTH INFORMATION

We make every effort to protect confidential health information whether it is written, electronic or oral. Some of the ways we comply with the Privacy Rule include:

- ☑ Papers containing confidential information, which are no longer required, are shredded.
- ☑ Our monitors are set up so passers-by cannot view confidential information that might be visible.
- ☑ We use screen savers that appear when the computer is not being used.
- ☑ We require users to log off when leaving their workstation.
- ☑ Oral communications with patients about their health care are conducted behind closed doors in private rooms.
- ☑ Oral communications with patients about their health care are conducted with discretion and every effort is made to avoid unauthorized person from overhearing the conversation. (lowered voices, facing the patient directly, etc.)
- ☑ The staff has been trained not to make any reference to a patients' health information in any area where the comments could be overheard.
- ☑ Our fax machine(s) is located in an area that is restricted to staff only.
- ☑ We verify fax numbers prior to sending any PHI.
- ☑ It is our policy never to leave sensitive information in our fax. If it is information that we are sending, it is returned to the file immediately. If it is information we receive, it is removed from the tray as soon as possible.

There are some situations where we are permitted to use and disclose PHI without a signed Authorization. Before any PHI is released under these circumstances we will verify the identity and authority of the individual who request the information.
Signed Authorizations are not required for:

- A patient's PHI can be disclosed to that patient on request
- A patient's PHI can be disclosed to a patient's personal representative only to the extent that it is relevant to the representative's capacity.
- It will not be released if we have reason to believe that such disclosure could cause harm to the patient or others
- Disclosures for public health activities
- Disclosures for health oversight agencies
- Disclosures to Federal officials for national security issues or lawful intelligence use
- Disclosures in response to subpoenas, court orders and other judicial processes
- Disclosures to law enforcement officials
- Disclosures to the military
- Disclosures required for reporting abuse, neglect or domestic violence
- Disclosures in response to federal or state laws
- Disclosures in response to the U.S. Department of Health and Human Services (HHS) request or compliance review
- Uses for marketing purposes that are limited to promotional gifts of a nominal value and/or face-to-face communications with a patient
- Effective March 26, 2013, immunization records for students may be released without an authorization (as long as the PHI disclosed is limited to proof of immunization). If an individual is deceased you may disclose PHI to a family member or individual involved in care or payment prior to death.

The use of a signed Consent Form is not required by HIPAA. Our policy on the use of Consent Forms is:

☑ This practice will not use Consent forms. The use of PHI for treatment, payment and healthcare operations is permitted by HIPAA.

☐ This practice elects to use signed Consent forms. We will make a good faith effort to obtain a signed Consent on the patient's first visit, or if already a patient, on the next visit.

- ☐ This practice is required by state law to obtain a signed Consent. We will make a good faith effort to obtain a signed Consent on the patient's first visit, or if already a patient, on the next visit.
- ☐ If we elect to use Consents, or if state law requires them, we recognize that there may be exceptions.

We will not require Consent in an emergency situation, if law requires the treatment or if there are communication problems that prevent us from obtaining Consent.

NON-ROUTINE DISCLOSURES

Patients have the right to know what non-routine uses or disclosures of their healthcare information have been made. Patients are advised of this right in our Notice of Privacy Practices. As required by HIPAA, we will maintain a log of all non-routine disclosures that includes information on:

- The date the request was received
- The date the information was released
- The name of the person or entity requesting the information
- Their address, if known
- The purpose for which the information will be used
- If an authorization or written notice was required and, if so, that the authorization or notice is current
- The name of the person authorizing the release

This log will be maintained for 6 years. If patients request a list of non-routine disclosures, it will be provided to them on the form, List of Non-Routine Disclosures. They have the right to know what information was released, to whom it was released and the purpose for which the information was used.

With the increasing use of Electronic Medical Record technology (EMR), the HITECH Act allows patients' the right to request a copy of your health information in electronic form if we store it electronically. If for some reason we aren't capable of an electronic format, a format requested by the patient or hardcopy will be provided.

PATIENTS' RIGHTS TO ACCESS AND AMEND THEIR HEALTH INFORMATION

As required by HIPAA and as stated in our Notice of Privacy Practices, patients have the right to review their health information and to amend that information. We will honor these rights.

Right of Access to PHI

- ☑ It is our policy to permit patients, or their personal representatives, the right to request access to their PHI.

- ☑ With rare exceptions, requests must be made in writing and are subject to review prior to granting, or denying, access.
- ☑ We reserve the right to deny access under circumstances allowed under the Privacy Rule.
- ☑ It is our policy to allow access only under the supervision of a member of our staff.

Right to Amend PHI

- ☑ Patients, or their personal representatives, have the right to request that their PHI be amended. We require that the request be made in writing.
- ☑ We will review all Requests to Amend and will permit amendments under guidelines established in the Privacy Rule.
- ☑ If the request is denied under provisions of the Privacy Rule, we will notify the patient, or the patient's representative, in writing and inform them of the reason or reasons for denial. They will be advised of their right to file a statement of disagreement and their right to file a complaint.
- ☑ If the request to amend is accepted, we will notify the patient, or the patient's representative, in writing of the decision. The amendment will be attached as a permanent document in the patient's record. We will notify business associates and others who might be affected by the amended or corrected information.

Right to Request Restriction

- ☑ Effective March 26, 2013, if patients' pay in full out of pocket for treatment, they can instruct us not to share information about the treatment with their health plan; if the request is not required by law.

RIGHT TO FILE A COMPLAINT

- ☑ This practice has established policies that allow patients the right to complain about our failure to comply with our Privacy Policies and Procedures, our Notice of Privacy Practices or the Privacy Rule. Patients are required to file complaints in writing. Upon receipt we will immediately investigate the complaint and, if valid, will make every effort to correct the problem. We will inform the patient of our action and will not retaliate against any patient who files a complaint.

- ☑ We encourage our staff to let our Privacy Officer, or management, know if they observe any failure to comply with our Privacy Policies and Procedures, our Notice of Privacy Practices or the Privacy Rule. We will not retaliate against any employee who files a complaint.

BREACH NOTIFICATION RULE / OMNIBUS RULE

As required by The American Recovery and Reinvestment Act of 2009, effective September 23, 2009, this practice will notify individuals whose PHI has been acquired, accessed, used or disclosed in an unauthorized manner. The Breach Notification Rules apply only if all of the following are present:

- There is a **"Breach"**. Effective March 26, 2013, it is a presumption that any acquisition, access, use or disclosure of PHI is a breach unless we can demonstrate that there is a low probability that the PHI has been compromised based on a 4 factor risk assessment. The rule defines "Breach" to mean the unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of the PHI.

- The PHI is **"Unsecured"**. The rule defines "Unsecured Protected Health Information" to mean PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by HHS guidance.

If all the above conditions above apply, we will use the form Security Breach Risk Assessment to determine if the PHI has been compromised. If a breach has occurred, Notification to the Secretary of HHS of a Security Breach of Unsecured Protected Health Information (located in the forms section of this manual) will be completed.

If more than 500 individuals are involved in the breach, then we will notify Health and Human Services concurrently with the individual notifications. For breaches involving fewer than 500 individuals, we will maintain an internal log or other documentation of such breaches and annually submit our log to HHS no later than 60 days after the end of each calendar year.

Effective March 26, 2013 increased penalties for improper disclosures:

VIOLATION TYPE	EACH VIOLATION	REPEAT VIOLATIONS/YR
Did Not Know	**$100-$50,000**	**$1,500,000**
Reasonable Cause	**$1,000-$50,000**	**$1,500,000**
Willful Neglect Corrected	**$10,000-$50,000**	**$1,500,000**
Willful Neglect Not Corrected	**$50,000**	**$1,500,000**

BUSINESS ASSOCIATES / SUBCONTRACTORS

This practice will obtain written agreements, or contracts, from our Business Associates that assure us that they will have a plan to safeguard all PHI received, created or maintained by them on behalf of this practice. Their use and disclosure of PHI is limited to the minimum necessary required for the performance of their contracted activities.

The terms of the contract we use conform to HIPAA and HITECH Act requirements. We reserve the right to terminate any such agreement or contract if we have reason to believe that the Business Associate has breached or violated the terms of the contract.

Effective March 26, 2013, all subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information.

MINIMUM NECESSARY

This practice will apply the "minimum necessary" standard to all aspects of our compliance with the Privacy Rule with few exceptions. The exceptions to the minimum necessary include:

- Information used by our staff for treatment purposes.
- Information disclosed to other healthcare professionals for treatment purposes.
- Information released in response to a valid authorization.
- Information required by HHS when required for compliance or enforcement of privacy regulations.
- Information required in order to comply with federal or state laws.

TRAINING

☑ It is the policy of this practice to train our staff on our Privacy Policies and Procedures. They will be advised of their obligations and responsibilities to protect patient healthcare information.

☑ We have developed appropriate discipline policies and will impose sanctions on staff members who violate our Privacy Policies and Procedures, the Privacy Rules, and other applicable privacy laws.

☑ All staff members are required to sign a Confidentiality Statement agreeing to abide by our Privacy Policies and Procedures.

☑ We train new employees within a reasonable period of time after hire and to each employee whose functions are affected by a material change in the policies and procedures, within a reasonable period of time after the material change becomes effective.

☑ It is our policy to train the entire workforce, including management, on security issues respective to our organizational uniqueness. We periodically provide security training updates based on technology and security risks and use Security reminders. We keep **Training records for 6 years.**

CHANGES TO PRIVACY POLICIES AND PROCEDURES

If there are revisions to the Privacy Rule and other federal or state privacy laws, this plan will be updated accordingly. Our Notice of Privacy Practices, if affected, will be revised to reflect any significant changes. Our patients and staff will be advised of changes which affect them. Only Dr. Rodin has the authority to make changes.

COMPLIANCE WITH STATE AND FEDERAL LAWS

This practice will comply with the privacy laws of this state that involve greater protection of healthcare information than the federal Privacy Rule.