

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

Doug Simpson CPA is a healthcare consultant, specializing in financial reporting; accounting operations, and compliance risk and control work with a special interest in revenue cycle process improvement, cost containment initiatives, and CMS value-based-purchasing compliance initiatives.

This Paper was prepared as a service to the public and is not intended to grant rights or impose obligations. The information is only intended to be a general summary. It is not intended to take the place of either the written law or regulations. We encourage readers to review the specific statutes, regulations, and other interpretive material for a full and accurate statement of contents.

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

Section One: Standards of Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy	Description	OCR/HIPAA Privacy Reg.
1000	General Administrative Requirements.	45 CFR 164.530
1100	Privacy Officer	45 CFR 164.530(a)(1)
1200	Policies and Procedures	45 CFR 164.530(i)(1)-(5)
1300	Initial Orientation and Training	45 CFR 164.530(b)(1)
1310	Training Members of the workforce on Revised Procedures	45 CFR 164.530(b)(2)(i)(C)
1400	Safeguards	45 CFR 164.502(a)(1)(iii) 45 CFR 164.502(b)(1) 45 CFR 164.514(d) 45 CFR 164.530(c)(1)
1500	Complaint Process	45 CFR 164.530(d)(1)
1510	Communicating the Complaint Process	45 CFR 164.530(d)(1) 45 CFR 164.520(b)(vi)
1520	Submitting Concerns and Complaints	45 CFR 164.530(d)(1) 45 CFR 164.520(b)(vi)
1530	Possible Violations of Privacy Policies	45 CFR 164.530(g)(1) 45 CFR 164.530(g)(2)(i-iii)
1540	Complaints About the Privacy Policies	45 CFR 164.530(d)(1)
1600	Staff Compliance and Sanctions	45 CFR 164.530(e-f)
1700	Mitigation Process	45 CFR 164.530(f)
1800	Waiver of Privacy Rights	45 CFR 164.530(h)(1)
1810	Refraining from Intimidating or Retaliatory Acts	45 CFR 164.530(g)(1) 45 CFR 164.530(g)(2)(i-iii)
1900	Documentation and Recordkeeping	45 CFR 164.530(j)(1-2)
2000	Uses and Disclosures of Protected Health Information	45 CFR 164.502(a)(1-2) 45 CFR 164.502(b) 45 CFR 164.514(d-e) 45 CFR 164.528(a)
2005	Disclosures Requiring Patient Authorization	45 CFR 164.502(a) 45 CFR 164.508(b)
2010	Disclosures Requiring Verification	45 CFR 164.514(h)(1)
2015	Personal Representatives	45 CFR 164.502(g)(1)
2020	When it is Appropriate to Disclose Patient Information to Other Persons Involved in the Patient's Care	45 CFR 164.510(b)

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

2025	Business Associates	45 CFR 164.504(e)
2030	Permitted Uses and Disclosures to Carry Out Treatment and Collect Payment	45 CFR 164.502(c)
2035	Patient Scheduling Job Functions	45 CFR 164.502(b)(1)
2040	Insurance Verification, Referral Certification and Authorization Job Functions	45 CFR 164.502(b)(1)
2045	Patient Registration Job Functions	45 CFR 164.502(b)(1)
2050	Collection of Co-Payment and Deductible Job Functions	45 CFR 164.502(b)(1)
2060	Financial Counseling Job Functions	45 CFR 164.502(b)(1)
2070	Patient Encounter Job Functions	45 CFR 164.502(b)(1)
2080	Transmitting Medical Correspondence for Patient Care Purposes Job Functions	45 CFR 164.502(b)(1)
2090	Patient Check-Out Job Functions	45 CFR 164.502(b)(1)
2100	"Front-End" Day End Processing Job Functions	45 CFR 164.502(b)(1)
2110	Posting Patient Charges Job Functions	45 CFR 164.502(b)(1)
2120	Billing Patient Claims Job Functions	45 CFR 164.502(b)(1)
2130	Claims Adjudication Job Functions	45 CFR 164.502(b)(1)
3000	Notice of Privacy Practices for Protected Health Information	45 CFR 164.520(a)
4000	Rights of Individuals to Request Restrictions on Disclosing and Using Protected Health Information	45 CFR 164.522(a)(1-2)
4100	Rights of Individuals to Place Confidential Communication Requirements on Protected Health Information	45 CFR 164.522(b)(1)
4200	Designated Records Sets Subject to Access by Individuals	45 CFR 164.524(e)(1)
4210	Rights of Individuals to Insect and Copy Their Protected Health Information	45 CFR 164.524(a)(1-4)
4220	Denial of Access Review Procedures	45 CFR 164.524(a)(4)
4300	Right to Amend Patient Information	45 CFR 164.526(a)
4400	Right to an Accounting of Disclosures of Protected Health Information	45 CFR 164.528(a)

Section Two:
Section Three:

Initial Orientation Training Manual
Minutes of Board of Directors
Notice of Privacy Practice
Training Certification

Section Four:

45 CFR Parts 160 and 164, Regulation Text

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 1000: GENERAL ADMINISTRATIVE REQUIREMENTS

REGULATION: 45 CFR 164.530

OBJECTIVE: **Physician Practice** shall maintain an efficient and effective administrative oversight function to safeguard the privacy of patient health information in compliance with OCR/HIPAA Privacy Regulation 45 CFR Parts 160 and 164.

PROCEDURES:

1. **Privacy Official and Patient Contact Person.** The organization shall designate a Privacy Official who shall be responsible for the development and implementation of the Standards for Privacy of Individually Identifiable Health Information Policies and Procedures (45 CFR 164.530(a)(1)(i).) In addition, the organization shall designate a patient contact person who will be responsible for receiving complaints and providing additional information about matters outlined in its written notice to patients regarding the privacy of individually identifiable health information (45 CFR 164.530(a)(1)(ii).)
2. **Policies and Procedures:** The organization shall implement privacy policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, and other requirements of OCR/HIPAA Privacy Regulation 45 CFR Parts 160 and 164 (45 CFR 164.530(i)(1). In addition, the organization shall modify its privacy policies as appropriate and necessary to comply with changes in the law (45 CFR 164.530(i)(2).
3. **Training.** The organization shall train all members of its workforce with respect to protecting the privacy of protected health information (45 CFR 164.530(b)(1).)
4. **Safeguards.** The organization shall maintain appropriate administrative, technical and physical safeguards to protect the privacy of protected health information (45 CFR 164.530(c)(1).)
5. **Complaint Process.** The organization shall maintain a process for individuals to make complaints concerning the organization's policies and procedures or its compliance with such policies and procedures (45 CFR 164.530(d)(1).)
6. **Sanctions.** The organization shall have and shall apply appropriate sanctions against members of its workforce who fail to comply with the Standards for Privacy of Individually Identifiable Health Information Policies and Procedures (45 CFR 164.530(e)(1).)
7. **Mitigation.** The organization shall attempt to mitigate, to the extent practically possible, any harmful effect that is known to have occurred because of its improper use or disclosure of protected health information (45 CFR 164.530(f)(1).)
8. **Waiver of Rights or Refraining from Intimidating or Retaliatory Acts.** The organization shall not require an individual to waive its right to file a complaint as a condition of treatment (45 CFR 164.530(h)(1).) In addition, the organization shall not intimidate, threaten, coerce, discriminate against or take other retaliatory actions

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

against individuals who file complaints in accordance with these policies and procedures; who file complaints with regulatory agencies; who testify, assist, or participate in an investigation, compliance review, or hearing under Part C of Title XI; or who oppose any unlawful act or practice so long as the individual believes in good faith that the act or practice is unlawful, the manner of the opposition is reasonable and does not involve the disclosure of protected health information (45 CFR 164.530(g)(1) and (g)(2)(i-iii).)

9. **Documentation:** The organization shall maintain a permanent record retention system for all required privacy communication (45 CFR 164.530(j)(1).)

_____ **Effective Date:** _____

Physician Practice, Privacy Officer

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 1100: PRIVACY OFFICER

REGULATION: 45 CFR 164.530(a)(1) requires that a designated individual be responsible for establishing and implementing the Standards for Privacy of Individually Identifiable Health Information Policies and Procedures. This regulation also requires that a designated individual be responsible for handling privacy inquiries and complaints.

OBJECTIVE: The Privacy Officer shall be responsible for the administrative oversight function that safeguards the privacy of patient health information in compliance with OCR/HIPAA Privacy Regulation 45 CFR Parts 160 and 164.

PROCEDURES:

1. The Physicians shall designate one individual to serve as the organization's Privacy Officer on an annual basis.
 - 1.1 shall serve as the initial Privacy Officer for Physician Practice.
2. Although the Privacy Officer may delegate duties to other employees or contractors, the Privacy Officer shall be accountable for ensuring the following responsibilities are carried out:
 - 2.1 Serve as a knowledgeable resource of key requirements of the HIPAA Standards for Privacy of Individually Identifiable Health Information.
 - 2.2 Develop, implement and maintain Standards for Privacy of Individually Identifiable Health Information Policies and Procedures that comply with federal and state standards, implementation specifications and other requirements.
 - 2.3 Develop and conduct training programs on protecting private health information.
 - 2.4 Respond to employee and patient questions concerning privacy policies and procedures.
 - 2.5 Address complaints concerning privacy practices described in the Notice of Privacy Practices.
 - 2.6 Address violations of Standards for Privacy of Individually Identifiable Health Information Policies and Procedures.
 - 2.7 Maintain a secure documentation retention program.

Effective Date: _____

Physician Practice, Privacy Officer

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 1200: POLICIES AND PROCEDURES

REGULATION: 45 CFR 164.530(i)(1) requires that the organization document and implement reasonable policies and procedures to comply with the federal privacy standards (OCR/HIPAA Privacy Regulation 45 CFR Parts 160 and 164.)

REGULATION: 45 CFR 164.530(i)(2) requires that these policies and procedures must be updated as changes occur in the federal privacy standards.

REGULATION: 45 CFR 164.530(i)(3) requires that these policies and procedures must be promptly updated when changes occur in the law that requires such changes.

REGULATION: Unless an earlier effective date is mandated by law, 45 CFR 164.530(i)(4) requires that material changes to the organization's privacy practices cannot be implemented until such time as a Revised Notice of Privacy Practices is issued to patients.

REGULATION: 45 CFR 164.530(i)(5) requires that these policies and procedures must be maintained in written or electronic copy, and the documents shall be retained for six years from the date of their creation or the date when they were last in effect, whichever is later.

OBJECTIVE: The organization's privacy practices shall be documented in writing and they shall remain consistent with the federal privacy standards and other relevant laws, and with its Notice of Privacy Practices.

PROCEDURES:

1. The Privacy Officer shall be responsible for outlining for the Physicians privacy practice requirements mandated by federal privacy standards and other relevant laws in the form of suggested policies and procedures, and when required, suggested revisions to the Notice of Privacy Practices.
2. The Physicians shall approve policies and procedures and the Notice of Privacy Practices before the organization implements changes to its privacy practices. These documents shall be maintained as part of the record retention system for privacy documents, and shall be retained in written or electronic form for a period not less than six years from the date of their creation or the date when they were last in effect, whichever is later.
3. The Physicians shall establish the effective date of policies and procedures and the Notice of Privacy Practices. When a change in privacy practices requires a change in the organization's Notice of Privacy Practices, the effective date of change cannot occur until such time as patients have been properly informed in writing of such changes.

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

4. The Privacy Officer shall be responsible for communicating and implementing the Physician approved privacy practice actions.
5. The Privacy Officer shall be responsible for maintaining updated copies of the Standards for Privacy of Individually Identifiable Health Information Policies and Procedures Manual in readily accessible locations for the front-office staff, the business office staff, and the medical staff.

Effective Date: _____

Physician Practice, Privacy Officer

DOUG SIMPSON, CPA

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 1300: INITIAL ORIENTATION AND TRAINING

REGULATION: 45 CFR 164.530(b)(1) requires that all members of the organization's workforce maintain a working knowledge of their individual responsibilities regarding the organization's privacy policies and procedures.

OBJECTIVE: All members of the workforce shall be equipped with the tools, resources and training required to carry out the privacy practices of the organization during their daily work routine.

PROCEDURES:

1. The Privacy Officer shall be responsible for providing all members of the workforce with access to the tools, the resources and the training requisite to carrying out the privacy practices of the organization.
2. The Privacy Officer shall develop and maintain a privacy policy orientation and training program. All members of the workforce are required to complete the initial program prior to April 14, 2003. All members entering the workforce after April 14, 2003 shall complete the initial training within their 90-day probation period.
3. After April 14, 2003, supervisors are responsible for the proper use and disclosure of private health information handled by their probationary employees.
4. The Initial Privacy Policy Orientation and Training Program shall be documented in writing, shall be retained in written or electronic form for a period not less than six years from the date of its creation or the date when it was last in effect, whichever is later, and at a minimum, shall cover the following elements:
 - 4.1 Definition and identification of protected health information.
 - 4.2 Notice of Privacy Practices form that is provided to all patients.
 - 4.3 Use and disclosure of protected health information for treatment, payment, and healthcare operations.
 - 4.4 Obtaining consent and authorization for use and disclosure of protected health information.
 - 4.5 Procedures for handling suspected violations of privacy policies and procedures.
 - 4.6 Penalties for violations of privacy policies and procedures.
 - 4.7 Documentation required by the policies and procedures manual.
5. The Privacy Officer shall be responsible for documenting that all members of the workforce have completed the Initial Privacy Policy Orientation and Training Program prior to April 14, 2003. For all members entering the workforce after April 14, 2003, the Privacy Officer shall be responsible for documenting that new members of the workforce have completed the Initial Privacy Policy Orientation and Training within their 90 day probation period.

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

- 5.1 Each member of the organization shall complete an Initial Privacy Policy Orientation and Training form documenting the date that they completed the orientation training, and acknowledge by signature that they have reviewed and understand the Standards for Privacy of Individually Identifiable Health Information Policies and Procedures Manual as it relates to their specific job duties and responsibilities.
- 5.2 Before a new hire is released from their probation period, the Privacy Officer or assignee shall acknowledge by signature that they have reviewed the orientation material and the Standards for Privacy of Individually Identifiable Health Information Policies and Procedures Manual with the new member of the workforce and the new member is prepared to perform his/her job duties in accordance with the Standards for Privacy of Individually Identifiable Health Information Policies and Procedures.
- 5.3 When the Initial Privacy Policy Orientation and Training form has been completed, the Privacy Officer will sign the form and place the form in the member's permanent employee record.

Effective Date: _____

Physician Practice, Privacy Officer

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

**PRIVACY RULE
TRAINING CERTIFICATION**

1. NAME : _____

2. JOB TITLE: _____

3. TYPE OF TRAINING PROVIDED:

I CERTIFY THAT I HAVE COMPLETED THE REQUIRED HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY RULE TRAINING SESSION DESCRIBED ABOVE. I FURTHER CERTIFY THAT I WILL ABIDE BY ALL OF THE POLICIES AND PROCEDURES PRESENTED IN ORDER TO ENSURE THE PROTECTION OF THE PROTECTED HEALTH INFORMATION (PHI) OF PATIENTS THAT I MAY ENCOUNTER WITHIN THE COURSE OF MY EMPLOYMENT AT PHYSICIAN PRACTICE.

EMPLOYEE'S SIGNATURE

DATE

PRIVACY OFFICIAL'S SIGNATURE

DATE

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 1310: TRAINING MEMBERS ON REVISED PROCEDURES

REGULATION: 45 CFR 164.530(b)(2)(i)(C) requires that members who are effected by a change in policy and procedure must receive adequate training in a reasonable time after the material change becomes effective and the training must be documented.

OBJECTIVE: The Privacy Officer shall be diligent in updating members of the workforce on changes to the Privacy Rule, and how those changes may affect their job functions.

PROCEDURES:

1. Upon receipt of the Physicians approval, the Privacy Officer shall provide members of the workforce with written documentation describing the new policy and procedures, the purpose for the changes in existing procedures, the effective date of the new policy and procedures, the type and means of training required, and the members who will be required to complete the training.
2. The documentation described in paragraph (1.) of this policy shall be retained in the record retention system for privacy documents in written or electronic form for a period not less than six years from the date of its creation.
3. Training shall normally be completed prior to the effective date of the new policy, but in no case shall be completed more than 30 days past the effective date. Supervisors are responsible for the proper use and disclosure of private health information handled by their employees who have not completed required training prior to the effective date.
4. The Privacy Officer shall be responsible for documenting that all effected members of the workforce have completed the Training Program prior to the designated effective date of the new or revised policies and procedures.
 - 4.1 The Privacy Officer will establish a "Training Form" to document training requirements for revised procedures. A copy of the approved policy and procedures will be attached to the Training Form. Listed below is a summary of the information included on the Training Form:
 - 4.1.1 Name and HIPAA policy number reference related to the training program.
 - 4.1.2 Description of training elements.
 - 4.1.3 Effective date that training must be completed.
 - 4.2 Members who are required to complete the training shall document the date that they completed the training program, and acknowledge by signature that they have reviewed and understand the revisions to the Standards for Privacy of

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

Individually Identifiable Health Information Policies and Procedures Manual as it relates to their specific job duties and responsibilities.

- 4.3 The Privacy Officer or assignee shall acknowledge by signature that they have reviewed the training program elements and the revised Standards for Privacy of Individually Identifiable Health Information Policies and Procedures Manual with the member of the workforce and the member is prepared to perform his/her job duties in accordance with the revised Standards for Privacy of Individually Identifiable Health Information Policies and Procedures.
- 4.4 When the Training Form has been completed, the Privacy Officer will sign the form and place the form and the attached policy and procedures in the member's permanent employee record.

Effective Date:

Physician Practice, Privacy Officer

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 1400: SAFEGUARDS

REGULATION: 45 CFR 164.502(a)(1)(iii) permits certain incidental uses and disclosures that occur as a by-product of another permissible or required use or disclosure, as long as reasonable safeguards have been applied and the minimum necessary standard as been implemented.

REGULATION: 45 CFR 164.502(b)(1), 164.514(d) requires that standards be established to provide reasonable assurance that protected health information will only be used or disclosed when it is necessary to satisfy a particular purpose or carry out a function.

REGULATION: 45 CFR 164.530(c)(1) requires that appropriate administrative, technical and physical safeguards be in place to protect the privacy of protected health information.

REFERENCE: OCR HIPAA Privacy, December 3, 2002, pages 11 - 20, Incidental Uses and Disclosures.

OBJECTIVE: Physicians, Nursing Staff and Business Office Staff shall analyze their own needs and circumstances related to the nature of the protected health information they hold, and shall assess the potential risks to patients' privacy. Reasonable precautions shall then be taken each day to limit the incidental use or disclosure of this information as further defined HIPAA Policy Section 2000. Examples of reasonable precautions are outlined in the following procedures.

PROCEDURES:

- 1 Medical records and billing records shall be maintained in an organized manner and shall be stored and used in work areas that are not easily accessible to the public or the general patient population.
 - 1.1. For purposes of patient care, as long as reasonable safeguards are in place, the patient chart may be stored outside of exam rooms prior to the patient visit. Examples of reasonable safeguards include limiting access to the exam room area, ensuring that the area is supervised, escorting non-employees in the area, and placing the patient chart in its holder with identifying information facing the wall or otherwise covered.
- 2 Medical records or billing records shall only be removed from their primary storage area to satisfy a particular purpose or carry out a specific function in the course of providing patient care or completing business operations.

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

- 2.1 When protected health information is removed from its primary storage area, reasonable safeguards shall be followed to protect patient privacy. For example,
 - Protected health information shall not be left unattended. Unattended information shall be locked in a filing cabinet or in a locked room, or it shall be returned to the primary storage area.
 - Computers shall not be left unattended. When an employee leaves his/her workstation, the employee shall log off the computer system.
 - When employees are required to engage the general public or patient population while working with this information, visual access to computer screens shall be restricted from their view and identifying information on medical records or billing records shall be covered.
- 3 Physician Practice shall use a patient sign-in sheet to register patients and shall call out patient names in the waiting area. However, the patient sign-in sheet will not include information pertaining to the medical problem for which the patient is seeing the physician.
- 4 Unless a patient has made a reasonable request that the physician office communicate with him/her in a confidential manner, the physician office staff can communicate with patients at their home through telephone or mail.
 - 4.1 Messages may be left on answering machines. A message related to appointment notification shall be limited to name, number, and other information necessary to confirm an appointment or a request that the individual return the phone call. A message related to any other medical or business purpose shall be limited to name, number and a request that the individual return the phone call.
 - 4.2 Messages may be left with a family member or other person who answers the phone when the patient is not at home. Use professional judgment to assure that such disclosures are in the best interest of the patient, and the message is limited to name, number, and other information necessary to confirm an appointment, or to ask that the patient return the phone call.
 - 4.3 Postcards may be used when mailing appointment reminders.
- 5 Facsimile machines shall be located in areas of the clinic practice that are not accessed by the general public. Telephone numbers and email addresses shall be confirmed before documents are transmitted electronically via facsimile or Internet. When these safeguards are followed, members of the workforce may electronically transmit and receive protected health information to and from authorized individuals.
- 6 Physicians, Nurses and Clinical Staff (Healthcare Providers) are always free to engage in communications as required for quick, effective, and high quality medical treatment. When the patient is present and coherent to make health decisions, and other people are present with the patient, request the patient's permission to disclose their health information in the presence of others. If the patient denies the request,

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

ask the people who have accompanied the patient to the exam room or who are in the hospital room to adjourn to the waiting room or another comfortable area.

As a normal practice, when other people are present in the general area that protected information is discussed, reasonable precautions should be taken to limit the incidental use or disclosure of this information. Examples of reasonable precautions would include using lowered voices or talking apart from others when sharing protected health information while

- Orally coordinating services at nursing stations.
 - Discussing a patient's condition over the phone with the patient or another health care provider.
 - Discussing lab test results with a patient or other provider in a joint treatment area.
 - Discussing a patients' condition or treatment regimen after surgery or in the patient's semi-private room.
- 7 In the patient examination and treatment work areas, reasonable steps shall be taken to avoid the possibility that a conversation may be overheard when sharing protected health information. For example,
- Patients shall be escorted from the waiting room to the exam room or other treatment areas and to the patient check-out counter by a member of the medical staff.
 - Reasonable measures should be taken to segregate patients from other patients when completing the patient exam, when discussing the patient's plan of care, when issuing orders, or when scheduling procedures.
 - When the business office staff is checking out a patient at the checkout counter, the medical staff member escorting another patient to the checkout area should always ask the escorted patient to stand in a location visible to the check out person, but separate from the patient providing the checkout staff protected health information.
 - Physicians shall either complete their dictation in their offices, or in an area of the surgical clinic that is not normally trafficked by the general public or the office staff.
- 8 In the reception area, the patient check-out area, the financial counseling area, and the business office area, reasonable steps shall be taken to avoid the possibility that a conversation may be overheard when sharing protected health information. For example,
- Staff responsible for greeting and checking in patients shall be sensitive to a patient's privacy during each patient encounter. Whenever possible, call patients

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

up individually to openly discuss protected health information. When this is not possible, it is okay to ask other patients in a courteous and professional manner to stand a few feet back from the area being used to obtain protected health information.

- Staff responsible for greeting and checking out patients shall be sensitive to a patient's privacy during each patient encounter. Whenever possible, call patients up from the designated holding area to openly discuss protected health information. When this is not possible, it is okay to ask other patients in a courteous and professional manner to stand a few feet back from the area being used to check patients out.
- Staff responsible for financial counseling shall not conduct direct patient encounters in open areas. At a minimum, the patient or patient representative should be segregated from other patients or staff members in a cubicle area that affords a level of privacy.
- Business operations functions shall not be conducted in unsupervised work areas directly accessible to the public or general patient population. As a minimum standard, business office functions should be segregated from patients or staff members in a cubicle area that affords a level of privacy.
- Telephone calls requiring the use or disclosure of protected health information shall not be made in areas normally accessed by the general public.

Effective Date: _____

Physician Practice, Privacy Officer

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

HIPAA Policy 1500: COMPLAINT PROCESS

REGULATION: 45 CFR 164.530(d)(1) requires an organization to maintain a process for individuals to make complaints concerning the organization's standards of privacy of individually identifiable health information policies and procedures or its compliance with such policies and procedures.

OBJECTIVE: Physician Practice shall maintain an open process for individuals to file complaints concerning its standards of privacy of individually identifiable health information policies and procedures or its compliance with such policies and procedures. Each complaint shall be taken seriously, shall be investigated appropriately, shall be mitigated when required, and the individual filing the complaint will be treated with courtesy and respect during and after the complaint process.

PROCEDURES:

1. The Privacy Officer shall manage the complaint and mitigation process outlined in section 1500 of these policies and procedures.

_____ **Effective Date:** _____

Physician Practice, Privacy Officer

DOUG SIMPSON, CPA

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

HIPAA Policy 1510: COMMUNICATING THE COMPLAINT PROCESS

REGULATION: 45 CFR 164.530(d)(1) requires an organization to maintain a process for individuals to make complaints concerning the organization's standards of privacy of individually identifiable health information policies and procedures or its compliance with such policies and procedures.

REGULATION: 45 CFR 164.520(b)(vi) requires that each patient be notified of the process by which they can file a complaint when they believe the organization has violated their privacy rights.

OBJECTIVE: Physician Practice's Notice of Privacy Practices shall include a section which shall notify patients and individuals of their right to file a complaint when they believe the organization has violated their privacy rights, and shall also describe the procedures by which the patient or individual may file his/her complaint.

PROCEDURES:

1. The Notice of Privacy Practices shall include a Complaint Section. An example of the type of language included in this section follows:

We are very concerned about protecting our patients' privacy rights, and are always interested in your comments and concerns. If you would like to submit a comment or a complaint regarding our current privacy practices, we encourage you to do so by sending a letter outlining your concerns to:

**Street Address
Austin, Texas 78705**

If you believe that your privacy rights have been violated, please do not hesitate to call the matter to our attention by sending a letter describing the cause of your concern to the same address.

_____ **Effective Date:** _____

Physician Practice, Privacy Officer

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 1520: SUBMITTING CONCERNS OR COMPLAINTS

REGULATION: 45 CFR 164.530(d)(1) requires an organization to maintain a process for individuals to make complaints concerning the organization's standards of privacy of individually identifiable health information policies and procedures or its compliance with such policies and procedures.

REGULATION: 45 CFR 164.520(b)(vi) requires that each patient be notified of the process by which they can file a complaint when they believe the organization has violated their privacy rights.

OBJECTIVE: Members of the workforce shall always be sensitive to patient privacy, and are encouraged to express concerns and suggest means to simplify or improve processes. Anyone expressing a concern or complaint shall always be taken seriously, and shall always be treated with dignity and respect. Patients and members of the workforce shall be directed to use the procedures defined below:

PROCEDURES:

1. Complaint forms shall be maintained at the Patient Registration desk and the Privacy Officer's office.
2. If a patient asks a member of the workforce how to file a complaint, the member shall provide the patient with a complaint form and a copy of the Notice of Privacy Practices, and shall inform the patient that they may contact the Privacy Officer directly by completing the form or writing a letter and either leaving it with staff at the patient registration desk or by mailing it to the address posted on the Notice of Privacy Practices.
3. When a member of the workforce receives a complaint which either involves a suspected violation of standards of privacy of individually identifiable health information policies and procedures or federal or state law, or they witness a suspected violation themselves, they shall immediately refer the complaint to the Privacy Officer for disposition in accordance with HIPAA Policy 1530. If the violation involves the Privacy Officer, the complaint shall be referred to a member of the Physician group for disposition in accordance with the same policy.
4. Members of the workforce shall normally express suggestions or concerns to their supervisor for disposition in accordance with HIPAA Policy 1540.

Effective Date: _____

Physician Practice, Privacy Officer

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 1530: POSSIBLE VIOLATIONS OF PRIVACY POLICIES

REGULATION: 45 CFR 164.530(d)(1) requires an organization to maintain a process for individuals to make complaints concerning the organization's standards of privacy of individually identifiable health information policies and procedures or its compliance with such policies and procedures.

REGULATION: (45 CFR 164.530(g)(1) and (g)(2)(i-iii)) states that the organization shall not intimidate, threaten, coerce, discriminate against or take other retaliatory actions against individuals who file complaints in accordance with these policies and procedures; who file complaints with regulatory agencies; who testify, assist, or participate in an investigation, compliance review, or hearing under Part C of Title XI; or who oppose any unlawful act or practice so long as the individual believes in good faith that the act or practice is unlawful, the manner of the opposition is reasonable and does not involve the disclosure of protected health information.

OBJECTIVE:

Members of the workforce may oppose any unlawful act or practice so long as the individual believes in good faith that the act or practice is unlawful, the manner of the opposition is reasonable and it does not involve the disclosure of protected health information.

When a member of the workforce receives a complaint which either involves a suspected violation of standards of privacy of individually identifiable health information policies and procedures or federal or state law, or they witness a suspected violation themselves, they shall immediately refer the complaint to the Privacy Officer for disposition in accordance with this policy. If the violation involves the Privacy Officer, the complaint shall be referred to a member of the Physician group for disposition in accordance with the same policy.

The Privacy Officer shall take each complaint seriously, and shall dispose of the complaint judiciously in accordance with the procedures defined below.

PROCEDURES:

1. The Privacy Officer shall evaluate each complaint and determine whether a violation has occurred, and if so, whether federal or state privacy laws and standards may have been violated, or whether the policies and procedures defined in this manual have been violated.
2. If the Privacy Officer determines that federal or state privacy laws and standards may have been violated, the Privacy Officer shall immediately forward the complaint to Physician Practice's legal counsel for evaluation. The request for legal evaluation

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

should specify a completion date. The Privacy Officer shall track the referral to timely completion. If the legal conclusion is that a federal or state privacy standard or legal requirement has been violated, the Privacy Officer shall complete the mitigation procedures outlined in HIPAA Policy 1700.

3. If the Privacy Officer determines that federal or state laws and standards have not been violated, a determination shall be made whether policies and procedures defined in this manual have been violated. If the conclusion is that a violation has occurred, the Privacy Officer shall complete the disciplinary procedures outlined in HIPAA Policy 1600.
4. As a normal practice, the Privacy Officer shall complete the evaluation process within 30 days. Upon completion of the evaluation process, the Privacy Officer shall notify the person submitting the complaint of the actions that will be taken to address the complaint.

Effective Date: _____

Physician Practice, Privacy Officer

DOUG SIMPSON, CPA

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 1540: COMPLAINTS ABOUT THE PRIVACY POLICIES

REGULATION: 45 CFR 164.530(d)(1) requires an organization to maintain a process for individuals to make complaints concerning the organization's standards of privacy of individually identifiable health information policies and procedures or its compliance with such policies and procedures.

OBJECTIVE: Each complaint shall be treated with dignity and respect, and shall be thoughtfully disposed of in accordance with the procedures defined below.

PROCEDURES:

1. The Privacy Officer shall review all complaints submitted in writing to Physician Practice.
2. The Privacy Officer shall normally assign a member of the workforce (Reviewer) to evaluate specific details of the complaint and determine whether corrective measures are necessary to address the underlying issues outlined in the complaint. Corrective action could include revising policies and procedures, establishing additional physical safeguards, or facilitating additional training for members of the workforce.
3. When the evaluation is complete, a written summary shall be provided to the Privacy Officer. The written summary shall include the steps taken to evaluate the specific details of the complaint, a listing of direct findings, and when required, a suggested course of action needed to address underlying issues outlined in the complaint.
4. When the evaluation is completed, and the Privacy Officer determines that changes are required, the Privacy Officer shall submit a written response to the person making the complaint. The written response shall include an expression of appreciation for the person's interest, an indication that a formal evaluation has been completed and a statement that the surgical practice believes that while its current practices comply with federal and state requirements, Physician Practice is considering changes in privacy practices, policies and procedures to address the person's concerns.
5. When the evaluation is completed, and the Privacy Officer determines that changes are not required, the Privacy Officer shall submit a written response to the person making the complaint. The written response shall include an expression of appreciation for the person's interest, an indication that a formal evaluation has been completed and a statement that the surgical practice believes that its current practices comply with federal and state requirements, and are sufficient to protect patient privacy.

_____ **Effective Date:** _____

Physician Practice, Privacy Officer

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 1600: STAFF COMPLIANCE AND SANCTIONS

REGULATION: 45 CFR 164.530(e) requires an entity to apply appropriate sanctions against staff members who violate its privacy policies and procedures.

REGULATION: 45 CFR 164.530(f) requires an entity to take practical measures to mitigate any harmful effects that arise from the use or disclosure of protected health information that violate policies and procedures in this manual, or requirements of federal or state law.

OBJECTIVE: Mistakes will occur when handling patient information which will result in protected information being released in an unauthorized manner. The objective is to provide Physician Practice the opportunity to mitigate those mistakes in a proactive manner.

What cannot be tolerated is behavior that results in a series or pattern of mistakes which result in the unauthorized release of medical record or billing record information.

What will not be tolerated are intentional acts which result in the unauthorized release of medical record or billing record information.

PROCEDURES:

1. Listed below is a summary of safeguards which when followed by staff members, should keep them in compliance with privacy policies and procedures:
 - Limit your disclosure of a patient's medical records or billing records to the specific amount required to complete your job assignment.
 - Limit discussions of patient information to those who are directly involved with you in the patient's treatment, payment or business operations activities, and conduct those conversations in a tone that is not readily overheard by other individuals in the area.
 - When you are required to contact a patient to notify them of an appointment, to communicate specific instructions provided by the physician, or to request billing information, make sure that you are calling the contact number or mailing to the contact address specifically provided by the patient.
 - If the patient is not available to accept a phone call, you may leave appointment information on the message machine or with a member of the family or other person involved in the patient's health care. In all other cases regarding communication of medical information or billing information, unless you are specifically instructed by a physician to do otherwise, simply leave a message for the patient to return your phone call.

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

- Limit Physician Practice requests of medical information and billing information to other health care providers and health plans to specific written instructions provided by the physician or specific written requirements established by the patient's health plan. Maintaining a copy of the physician order or a copy of the front and back of the insurance card in the patient chart should be sufficient to serve as a reasonable audit trail.
 - Limit disclosure of medical record or billing record information to situations related to treatment, payment and accounting activities. Before releasing patient information, document in writing the person's name, the organization's name, the medical purpose or payment purpose of the request, the specific information that is needed to fulfill the stated purpose, and the exact address Physician Practice shall use to transmit the information (Validation Record). If there is any question regarding the propriety of the request, seek instruction from the physician. The Validation Record, the fax cover sheet or cover letter, and a copy of the information submitted to the requesting party should be maintained in the patient's privacy record. This documentation should adequately serve as a reasonable audit trail.
 - When patient's request their records be forwarded to a third party, require the patient to submit the request in writing, specifying the information that is to be released, the timeframe or event associated with the release, the name and address of the person the patient authorizes to receive the information, and Physician Practice authority to release the information on behalf of the patient. Provide the request and the patient chart to the physician, and follow their specific instructions for handling the patient's request. The patient authorization, documentation of the physician's oral or written instruction, the fax cover sheet or cover letter, and a copy of the information submitted on the patient's behalf should be maintained in the patient's privacy record. This documentation should adequately serve as a reasonable audit trail.
 - Any other requests for disclosure of medical records or billing records shall be directed to a physician or the privacy officer for disposition. When their assistance is requested, their specific instructions must be followed.
 - When working with medical records or billing records, do not leave the information unattended or readily available for other people to observe.
 - When signed-on to the medical management information system, keep the monitor screen directed away from general traffic, and do not leave the computer station unattended.
2. When a staff member believes that they have violated a privacy policy and procedures, or they are aware of another member of the workforce whom they believe has violated a privacy policy and procedures, they should report the incident to a physician or the privacy officer. This conduct will allow everyone to work the potential problem together in a proactive manner, and this action will result in favorable treatment when sanctions are applied.

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

3. When staff members unintentionally use or disclose protected health information in violation of these privacy policies and procedures, the incident shall be documented in the staff member's personnel file. The privacy officer shall review the incident with the staff member and provide additional training as required to reasonably prevent another incident.
4. A pattern of repeated unintentional use or disclosure of protected health information in violation of these privacy policies and procedures shall result in either transfer to another position, suspension, or termination.
5. Flagrant disregard for these policies and procedures documented through a privacy officer investigation that is a violation of the Privacy Rule may result in termination of employment. The incident shall be documented in the staff member's personnel file. The privacy officer shall review the incident with the staff member and shall also review the incident with the Physicians. The Physicians will make a final determination of required conditions of future employment, or whether an employee shall be terminated.
6. Intentional disclosure of protected health information in violation of these policies and procedures that is discovered and documented through a privacy officer investigation may result in immediate suspension, pending further investigation and termination. Documentation of the incident must show clear evidence that the disclosure was intentional and deliberate. The incident shall be documented in the staff member's personnel file. The privacy officer shall review the incident with the staff member and shall also review the incident with the Physicians.

Effective Date: _____

Physician Practice, Privacy Officer

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

HIPAA Policy 1700: MITIGATION PROCESS

REGULATION: 45 CFR 164.530(f) requires an entity to take practical measures to mitigate any harmful effects that arise from the use or disclosure of protected health information that violate policies and procedures in this manual, or requirements of federal or state law.

OBJECTIVE: When legal counsel determines that federal or state standards or legal requirements may have been violated, legal counsel shall conduct all communications with the person filing the complaint regarding the complaint.

PROCEDURES:

1. When the Privacy Officer determines that actions described in a complaint have violated federal or state standards or legal requirements, the matter shall be turned over to Physician Practice's legal counsel to determine any action needed to mitigate any harm that may result to the patient; to evaluate legal exposure and recommend a course of action, and to follow up with the patient.

_____ **Effective Date:** _____

Physician Practice, Privacy Officer

DOUG SIMPSON, CPA

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

HIPAA Policy 1800: WAIVER OF PRIVACY RIGHTS

REGULATION: (45 CFR 164.530(h)(1) states that an organization cannot require an individual to waive its rights to file a complaint as a condition of treatment.

OBJECTIVE: No patient shall ever be asked to waive its rights to file a complaint as a condition of treatment.

PROCEDURES:

1. The Privacy Officer shall enforce this policy by sanctions outlined in HIPAA Policy 1600.

_____ **Effective Date:** _____

Physician Practice, Privacy Officer

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

**HIPAA Policy 1810: REFRAINING FROM INTIMIDATING OR RETALIATORY
ACTS**

REGULATION: 45 CFR 164.530(g)(1) and (g)(2)(i-iii) states that the organization shall not intimidate, threaten, coerce, discriminate against or take other retaliatory actions against individuals who file complaints in accordance with these policies and procedures; who file complaints with regulatory agencies; who testify, assist, or participate in an investigation, compliance review, or hearing under Part C of Title XI; or who oppose any unlawful act or practice so long as the individual believes in good faith that the act or practice is unlawful, the manner of the opposition is reasonable and does not involve the disclosure of protected health information.

OBJECTIVE: Patients, individuals and members of the workforce shall be treated in a considerate and professional manner in all circumstances related to the policies and procedures in this manual.

PROCEDURES:

1. The Privacy Officer shall enforce this policy by sanctions outlined in HIPAA Policy 1600.

_____ **Effective Date:** _____

Physician Practice, Privacy Officer

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 1900: DOCUMENTATION AND RECORDKEEPING

REGULATION: 45 CFR 164.530(j)(1) requires that a copy of all required written communications be retained by the organization in a hardcopy or electronic format.

REGULATION: 45 CFR 164.530(j)(2) wants all required documentation to be retained for a period of six years from the date of creation or the date written communication was last in effect, whichever is later.

OBJECTIVE: The Privacy Officer shall maintain an accurate record of all required written communication required by this policy and procedures manual in a secure environment. Listed below are examples of required written communication:

- The Physicians minutes designating the Privacy Officer for the initial year and the subsequent years (45 CFR 164.530(a)(2)).
- The Physicians minutes designating the contact person responsible for receiving patient complaints for the initial year and the subsequent years (45 CFR 164.530(a)(2)).
- The Physicians minutes approving the initial Notice of Privacy Practices and subsequent revisions to the original Notice of privacy Practices.
- The Notice of Privacy Practices (HIPAA Policy 3000).
- The Physicians minutes approving the initial Standards for Privacy of Individually Identifiable Health Information Policies and Procedures and subsequent additions or revisions to the original manual (45 CFR 164.530(i)(1) and (j)(1)(i)).
- The Standards for Privacy of Individually Identifiable Health Information Policies and Procedures (45 CFR 164.530(i)(2)(iii) and (j)(1)(i)).
- Training Program documentation (45 CFR 164.530(b)(2)(ii)).
- Documentation of sanctions that are applied, if any (45 CFR 164.530(e)(1)).
- Documentation of complaints received, and their disposition, if any (45 CFR 164.530(d)(2)).
- Documentation of unauthorized use or disclosure, and their disposition (45 CFR 164.502(a)(1)).
- Business Associate Agreements (45 CFR 164.504(e)).
- Patient confidentiality agreements documentation (HIPAA Policy 4100).
- Agreed-upon restrictions documentation (HIPAA Policy 4000).
- Patient request to inspect or copy medical or billing records documentation (HIPAA policy 4210).
- Patient request to amend protected health information documentation (HIPAA Policy 4300).

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

- Patient authorizations to disclose protected information to non-covered individuals or entities and support documentation (HIPAA Policy 2005).
- Written documentation obtained by members of the medical staff and business office staff, verifying an individual's authority to access protected health information; the purpose of the request for access; a description of requested information; and the transmission address before permitted information is transmitted to authorized recipients (HIPAA Policy 2010).
- Copies of disclosures pertaining to victims of abuse, neglect or domestic violence, and their required support documentation (HIPAA Policy 4400).
- Copies of disclosures pertaining to judicial and administrative proceedings, and their required support documentation (HIPAA Policy 4400).
- Copies of disclosures pertaining to law enforcement activities, and their required support documentation (HIPAA Policy 4400).
- Copies of disclosures pertaining to public health activities, and their required support documentation (HIPAA Policy 4400).
- Copies or disclosures pertaining to health oversight activities, and their required support documentation (HIPAA Policy 4400).
- Copies of disclosures pertaining to specialized government functions, and their required support documentation (HIPAA Policy 4400).
- Copies of disclosures pertaining to coroners and medical examiners, and their required support documentation (HIPAA Policy 4400).
- Copies of disclosures pertaining to funeral directors, and their required support documentation (HIPAA Policy 4400).
- Copies of disclosures pertaining to workers compensation insurance, and their required support documentation (HIPAA Policy 4400).
- Accounting to patients of disclosures of protected information made by the organization (45 CFR 164.528(d)).

PROCEDURES:

1. Written communication required by this policy is protected information, and shall be safeguarded under the Privacy Officer's supervision. Required documentation shall be maintained in hardcopy or electronic format, and shall be maintained for six years from the date of creation, or the last effective date, whichever is later.
2. Physician Practice shall maintain a permanent record retention system used for privacy documents.
3. General and administrative records shall be maintained in the permanent record retention system in such a manner as to readily document compliance with the Privacy Rule general and administrative requirements.
4. Patient privacy records shall be maintained in the permanent record retention system in individually designated record sets, and shall be maintained in such a manner to readily document compliance with the Privacy Rule's permitted disclosure of

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

protected health information, as well as to facilitate accounting to individuals of disclosures of their protected health information.

_____ **Effective Date:** _____

Physician Practice, Privacy Officer

DOUG SIMPSON, CPA

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 2000: USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

DEFINITIONS:

Business Associate: A business associate is not a member of the health care provider's workforce, but acts in the capacity of a member of the workforce to perform or assist in performing job functions involving the use or disclosure of individually identifiable health information. Examples could include contract billing and collection services, contract practice management services, contract financial services and accounting services, and legal services.

Designated Record Set: A designated record set means the medical records and billing records about individuals maintained by or for health care providers; and the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan (45 CFR 164.501).

Disclosure: Disclosure means the release, transfer, provision of access to, or divulging in any other manner protected health information outside the entity holding the information (45 CFR 164.501).

Health Information: Health information is any information whether oral or recorded in any form or medium that is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse that relates to the past, present or future physical or mental health or condition of an individual; the provision of healthcare to the individual; or the past, present, or future payment for the provision of healthcare to an individual (45 CFR 160.103).

Healthcare Operations: A limited example of healthcare operations would include quality assessment and improvement activities; training, accreditation, certification, licensing, and credential activities; contracting with health plan activities; medical review, legal services and audit activities; business planning and development related to managing and operating the business; and business management and general administrative activities of the business (45 CFR 164.501).

Individually Identifiable Health Information: Individually identifiable health information is health information and demographic information that is collected from an individual that readily identifies the individual or there is a reasonable basis to believe that the information can be used to identify the individual (45 CFR 160.103).

Payment: Payment means business office activities required to bill and collect reimbursement for services rendered (45 CFR 164.501).

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

Protected Health Information: Protected health information (Patient Health Information) is individually identifiable health information that is transmitted or maintained in any form or medium to include electronic media (45 CFR 164.501).

Workforce: Workforce means any person (paid or un-paid and W-2 or 1099) who works under the direct control of Physician Practice (45 CFR 160.103).

REGULATION: 45 CFR 164.502(a)(1) states that the organization is only permitted to use and disclose protected health information (medical, demographic or financial patient health information) for the purposes of

1. Direct patient contact (45 CFR 164.502(a)(1)(i)).
2. Treatment, payment or healthcare operations activities (*subject to exceptions associated with required authorizations or established agreements.*) (45 CFR 164.502(a)(1)(ii)(iv)(v) and 164.506 and 164.508 and 164.510).
3. Maintaining the facility directory or providing reasonable notification (45 CFR 164.510).
4. Compliance with the law (45 CFR 164.512(a)).
5. Compliance with public health authorities and other government activities authorities authorized to receive such information (45 CFR 164.512(b)).
6. Compliance with disclosures about victims of abuse, neglect, or domestic violence (45 CFR 164.512(c)).
7. Compliance with health oversight activities (45 CFR 164.512(d)).
8. Compliance with disclosures for judicial and administrative proceedings (45 CFR 164.512(e)).
9. Compliance with disclosures for law enforcement activities (45 CFR 164.512(f)).
10. Working with coroners or medical examiners to identify a deceased person, determine a cause of death, or other duties as authorized by law (45 CFR 164.512(g)).
11. Compliance with laws relating to workers compensation insurance 45 CFR 164.512(l).
12. Satisfying requests of Business Associates for information related to research, public health or healthcare operations which excludes data which would allow the user to identify the individual, or the individuals family members, relatives or employer (*subject to completion of a Data Use Agreement*) (45 CFR 164.514(e)).
13. Fund raising activities of the organization, a business associate, or an institutionally related foundation as long as the information is limited to demographic information and dates of service (*subject to Notice of Privacy requirements*) (45 CFR 164.514(e)).

REGULATION: 45 CFR 164.502(a)(2) states that the organization is normally required to provide an individual access to inspect and obtain a copy of his/her protected health information (164.524(a)(1); and is also required to provide individuals with an

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

accounting of disclosures of their protected health information that falls outside permitted use and disclosures of that information (164.528(a)).

REGULATION: 45 CFR 164.502(b) allows for the incidental use or disclosure of otherwise protected health information if the organization has made reasonable efforts to limit the amount of protected health information to the minimum standard required to accomplish the intended purpose of the use, disclosure, or request (164.502(b)(1)). For example,

1. The organization has identified individuals or classes of individuals (job title) in the workforce who need access to protected health information to carry out their duties, it has identified the types of protected health information to which access is necessary by job title and any conditions appropriate to such access, and the organization makes reasonable efforts to limit access based on assigned job duties and assigned access levels (164.514(d)); and
2. The organization does not use, disclose or request an entire medical record unless the entire medical record is specifically justified as the amount reasonably necessary to accomplish the purpose of the use, disclosure or request (164.514(e)).

OBJECTIVE: The organization shall only use and disclose protected health information that is permitted or required by the privacy regulations defined below, and it shall make reasonable efforts each business day to minimize the incidental use or disclosure of otherwise protected health information as further defined in this HIPAA Policy section 2000.

Listed below is a summary of protected health information that Physician Practice is permitted to use and disclose, and when required by the Privacy Rule, special conditions that must be met before a patient's health information may be accessed or released by members of the workforce:

- **Direct patient contact.** Patient health information may always be disclosed directly to the patient. However, two precautions must be observed.

When other people are in attendance, request the patient's permission to discuss their health information in the presence of others. If the patient objects, ask the people to leave in a professional or courteous manner.

When other people are in the general area, speak in a tone that can be clearly heard by the patient, but does not easily project to others.

- **Treatment, payment or healthcare operations activities.** Patient health information may be created or received to carry out treatment, payment and

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

healthcare operations activities. However, certain precautions must be observed when handling patient health information for these purposes.

Access to patient health information shall be limited to the information required for the workforce to complete its assigned job functions.

A patient sign in sheet shall be used by the clinic, but the information provided on the sheet shall be limited and shall not disclose medical information.

The patient's name shall be announced when calling the patient back to the exam area, but other personal references shall be limited when communicating with the patient directly or about the patient indirectly when other people are in the general area.

Make sure that confidentiality instructions are followed when attempting to contact the patient or when communicating with others for notification or payment purposes.

Make sure that agreed-upon restrictions to access are followed before using or disclosing patient health information.

Messages regarding appointment notification and messages to return calls to the physician office may be left on personal answering machines, or may be left directly with a closely identified individual when the patient is not present (see confidentiality instructions and agreed-upon restrictions for possible exceptions to this rule.)

Make sure that a valid authorization has been established before disclosing psychotherapy notes or disclosing patient health information for organized marketing purposes.

Document a requesting person's authority to access patient health information, the purpose of the access, and the transmission address before disclosing patient health information to other health care providers, health plans, or business associates.

- Disclosures pertaining to Victims of abuse, neglect or domestic violence (This section does not apply to suspected victims of child abuse or neglect.) Patient health information may be disclosed to government authorities who are authorized to receive reports of domestic violence, abuse and neglect. Certain conditions must be met before a physician releases such information:

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

Obtain written authorization from the victim or patient representative to release information that is limited to relevant requirements of the law.

If the individual is unable to agree because they are incapacitated, obtain written documentation from the government authority that the information will not be used against the patient, and that a law enforcement activity dependent on the patient health information would be materially and adversely affected by waiting until the patient is able to agree to the disclosure.

In all other cases, legal counsel shall be sought to ensure that the incident is required to be reported by law or is expressly authorized by statute or regulation before disclosing patient health information for these purposes. The patient or personal representative must be promptly informed that such action has been or will be taken, except when the physician believes that such knowledge would put the patient at risk of serious harm.

- Disclosures pertaining to Judicial and administrative proceedings. A physician in the course of any judicial or administrative proceeding may disclose patient health information. Certain conditions must be met before a physician releases such information:

The physician receives an order of the court or administrative tribunal, and only discloses that information expressly authorized by such order.

Without an order of the court, a physician can only respond to a subpoena, discovery request, or other lawful process when the following written assurances have been obtained from the requesting party:

- o A good faith attempt has been to provide notice to the patient or personal representative,
- o The notice provided sufficient information about the litigation or proceeding to permit the patient or personal representative to raise an objection, and
- o The time to raise an objection has elapsed, and
- o No objection has been filed or the court or administrative tribunal has resolved filed objections and the requested disclosure is consistent with the resolution.
- o A qualified order has been provided to the physician that documents that the protected information shall only be disclosed for the purposes of the litigation or proceeding for which it has been requested, and the protected information (including all copies) shall be returned or destroyed at the end of the litigation or proceeding.

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

- Disclosures pertaining to law enforcement activities.

Wounds and injuries: The physician shall disclose protected health information to meet legal reporting requirements of certain types of wounds or injuries.

Legitimate law enforcement inquiry: The physician shall disclose protected health information when provided written documentation establishing legal authority to access such information so long as the disclosure is relevant and limited to a legitimate law enforcement inquiry, the scope of the request is specific and limited, and de-identified information could not reasonably be used.

Identifying and locating individuals: Pursuant to a law enforcement official's request for the purpose of identifying or locating an individual, the physician may disclose the following patient health information: name and address; date and place of birth; social security number; ABO blood type and rh factor; type of injury; date and time of treatment; date and time of death, if applicable; and description of distinguishing physical characteristics.

Victim of crime: Patient health information may be disclosed in response to a law enforcement request when the patient is a suspected victim of a crime. Certain conditions must be met before a physician releases such information:

Obtain written authorization from the victim or patient representative to release information, or if the patient is unable to agree because of incapacity or other emergency circumstance, obtain written documentation from the law enforcement official that the information is needed to determine whether a crime has been committed against the victim and the information will not be used against the victim; that a law enforcement activity dependent on the patient health information would be materially and adversely affected by waiting until the patient is able to agree to the disclosure; and the physician believes that the disclosure is in the patient's best interest.

Decedents: The physician may disclose a decedent's protected health information to alert law enforcement officials when the physician suspects that the patient's cause of death was the result of criminal conduct.

Crime on premises: A physician may disclose to law enforcement officials protected health information that Physician Practice believes in good faith constitutes physical evidence of criminal conduct that occurred at their location.

Reporting crime in emergencies (This section does not apply to suspected victims of abuse, neglect or domestic violence.) If a physician renders medical aid in an emergency situation at a suspected crime scene, the physician may

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

- disclose protected information to alert law enforcement to the commission and nature of the crime; the location of the crime and the victim of the crime, and the identity, description, and location of the perpetrator of the crime.
- **Public health activities.** A physician may disclose protected information to a public health authority that is authorized to collect or receive information for the purpose of preventing or controlling disease, injury, or disability; or to a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect.
 - **Health oversight activities.** A physician may disclose protected health information to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, criminal proceedings or actions; or other activities necessary for appropriate oversight of:
 - Government benefit programs to determine beneficiary eligibility.
 - Government regulatory programs to determine compliance with program standards or civil rights laws.
 - **Specialized government functions.** A physician may disclose protected health information to facilitate the following government functions: military and veterans activities; national security and intelligence activities; protective services for the president and others; and medical suitability determinations for security clearance purposes.
 - **Correctional institutions and other law enforcement custodial situations.** A physician can disclose protected information about a patient in the custody of a law enforcement official when the following written assurances have been obtained from the requesting party that the disclosure is necessary for the provision of health care to the patient; for the health and safety of the patient and others involved in the patient's transportation or involved with the patient at the correctional or custodial facility; and for the administration and maintenance of the safety, security, and good order of the correctional facility.
 - **Coroners and medical examiners.** A physician may disclose protected health information to a coroner or medical examiner for the purposes of identifying a deceased person, determining a cause of death, or other duties as authorized by law.
 - **Funeral directors.** If it is necessary for the funeral director to carry out their duties, the physician may disclose protected health information prior to, and in reasonable anticipation of a patient's death.
 - **Workers compensation insurance.** A physician may disclose protected health information for the purpose of complying with laws relating to workers' compensation or other such programs established by law that provide benefits for work-related injuries or illness without regard to fault.

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

PROCEDURES:

1. Member of the workforce may create records, and access or disclose patient health information as defined above, and in accordance with the conditions stipulated in each of these sections and in the remainder of this HIPAA Policy Section 2000.
2. Documents obtained to verify authority to access protected information and copies of patient health information actually disclosed to individuals permitted by the Privacy Rule to access and use requested information as defined above shall be maintained in individual record sets of the record retention system established for privacy documents.
3. In all other cases where a patient's protected health information could be disclosed, members of the workforce must obtain a valid written authorization from a patient or patient's personal representative before disclosing a patient's protected health information.

Effective Date: _____

Physician Practice, Privacy Officer

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 2005: DISCLOSURES REQUIRING AUTHORIZATIONS

REGULATION: 45 CFR 164.502(a) outlines protected health information that health care providers are permitted to use and disclose without an individual's authorization.

REGULATION: 45 CFR 164.508(b) states that valid authorization is required to use or disclose psychotherapy notes or to use or disclose protected health information for most organized marketing purposes.

OBJECTIVES:

Members of the workforce shall not disclose protected health information that is not permitted or required to be disclosed by the Privacy Rule and as summarized in HIPAA Policy 2000 without first obtaining valid authorization from the individual.

Members of the workforce shall not request access to or disclose psychotherapy notes without valid authorization from the individual.

Members of the workforce may market the medical practice in face-to-face communication with an individual, and may use its database to send nominal gifts to its patient population (e.g., calendar, pens). Any other organized marketing activity utilizing individual health information maintained by the medical practice shall be managed by the Privacy Officer, and shall meet the requirements for valid authorization defined below.

PROCEDURES:

1. Authorizations must be documented in plain language, signed, and retained for six years in the record retention system for privacy documents. A copy shall be provided to the individual providing the authorization.
2. A valid authorization must include the following core elements:
 - A specific and meaningful description of the information to be used or disclosed.
 - A specific and meaningful description of whom or of who is able to use or disclose the information.
 - A description of each purpose of the requested use or disclosure. The statement, "at the request of the individual" is sufficient when the individual initiates the request, and the individual does not choose to provide a statement.
 - An expiration date or a specific and meaningful description of an expiration event.
 - A statement notifying the individual of their right to revoke the authorization in writing.

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

- When the authorization will be used to disclose marketing information, and the medical practice is to receive remuneration for providing the information, the authorization must include a statement to that effect.
- A signature and a date.

Effective Date: _____

Physician Practice, Privacy Officer

DOUG SIMPSON, CPA

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 2010: DISCLOSURES REQUIRING VERIFICATION

REGULATION: 45 CFR 164.514(h)(1) requires the health care provider to verify the identity of the person requesting protected health information and what authority they are acting under prior to disclosing protected health information to that person.

OBJECTIVE:

Protected health information shall not be released to other persons without identifying the person as a person with authority to have access to the information to carry out treatment, payment or health operations activities, or other activities permitted by the Privacy Rule. If an agreed-upon restriction has been placed on information used to carry out treatment, payment or health operations activities, this information cannot be disclosed outside the terms of the restriction.

PROCEDURES:

1. Medical records information or billing records information may be released without a written authorization from an individual to other people who are permitted by the Privacy Rule to use and disclose the individual's health information. For example, business associates, other health care providers, health care plans, personal representatives, law enforcement agencies, and governmental agencies are permitted to use protected health information in compliance with the Privacy Rule.
2. Before a member of the workforce releases medical information or billing information without an individual authorization, verify that a restriction has not been established to prohibit the disclosure. A copy of the agreed-upon restrictions and the physician instructions shall be retained in the patient chart, and a copy of the documents shall be retained in the permanent record retention system used for privacy documents. The physician instructions shall also be documented in a special instructions field of the medical management information system.
3. Before a member of the workforce releases medical information or billing information without an individual authorization, obtain written documentation which readily infers the name of the requesting person or entity, that person or entities authority to access the information, the purpose of the request, a description of the requested information, and the address members of the workforce shall use to transmit the information.
4. Written documentation shall be retained for six years in the permanent record retention system used for privacy documents.

_____ **Effective Date:** _____

Physician Practice, Privacy Officer

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 2015: PERSONAL REPRESENTATIVES

REGULATION: 45 CFR 164.502(g)(1) requires that health care provider treat persons with legal authority to act as a patient's legal personal representative as the patient/individual when using or disclosing protected health information. Exceptions to this general rule follow:

- An unemancipated minor has the authority to act as an individual; the minor has consented to the health care service, and the minor has not requested that the person be treated as the personal representative.
- An unemancipated minor may lawfully obtain health service without the consent of a parent, guardian, or other person acting *in loco parents*, and the minor or other legal authority has consented to the health care service.
- A parent, guardian, or other person acting *in loco parents* assents a confidentiality agreement.
- The health care provider determines through professional judgment that it is not in the best interest of the individual to treat a person as a personal representative

OBJECTIVE:

Legal authority to act as a personal representative shall be established within the patient record before a person other than the individual can be treated as the individual when disclosing protected health information.

PROCEDURES:

1. During the patient registration process, an unemancipated minor's parent or legal guardian shall sign the information sheet designating them self as the minor's personal representative.
2. In all other cases, a power of attorney or other legally acceptable form of documentation shall be secured and placed in the patient's chart before a person can be treated as the individual when disclosing protected health information.

Effective Date: _____

Physician Practice, Privacy Officer

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 2020: WHEN IT IS APPROPRIATE TO DISCLOSE PATIENT INFORMATION TO OTHER PERSONS INVOLVED IN THE INDIVIDUALS CARE

REGULATION: 45 CFR 164.510(b) states that when a patient is present and coherent they shall be afforded the opportunity to agree or object to the disclosure of protected health information to closely identified persons. When the individual is not present or does not have the capacity to make health care decisions, health care providers can use their professional judgment to determine when it is in the best interest of the individual to disclose protected health information to closely identified persons (close friends, family members, relatives, etc.). When it is in the individual's best interest, limited information can be disclosed that is directly relevant to that person's involvement in the individual's health care or in the payment related to the individual's health care.

OBJECTIVE:

If a patient is present and has the capacity to make health care decisions, the patient shall determine who can have access to the health information presented by the physician or medical staff. If an individual is not present, or is incapacitated or involved in an emergency circumstance, the physician shall determine when it is in the best interest of the individual to disclose protected health information to closely identified persons (close friends, family members, relatives, etc).

PROCEDURES:

1. Members of the medical staff and business office staff may use protected health information to notify a person responsible for an individual's care of the patient's location, their general health condition, or death.
2. If other individuals are present during a patient encounter, the patient's permission shall be requested before disclosing protected information. If an objection occurs, the situation shall be managed in a courteous and professional manner.
3. If the physician has agreed to restrict protected health information used to carry out treatment, payment or health operations activities, the restrictions shall be honored when communicating with closely identified persons.
4. Members of the medical staff shall follow specific physician instructions when communicating protected health information to others who are directly involved in the patient's healthcare.

Effective Date: _____

Physician Practice, Privacy Officer

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 2025: BUSINESS ASSOCIATES

REGULATION: 45 CFR 164.502(e) allows health care providers to disclose protected health information to a business associate and may allow the business associate to create or receive protected health information on its behalf, if it documents that it has obtained satisfactory assurance that the business associate will appropriately safeguard the information.

REGULATION: 45 CFR 164.504(e) states that the health care provider is in violation of the Privacy Rule if its business associate is involved in a pattern of activities that violate the Privacy Rule, and the health care provider becomes aware of the pattern of violations and does not take reasonable steps to stop the business associates non-compliance behavior.

OBJECTIVE:

Physician Practice may contract out health care operations functions to business associates that demonstrate an active knowledge of Privacy Rule compliance requirements and which provide documented assurances that they will comply with those requirements while using or creating protecting health information on our behalf.

PROCEDURES:

1. The Privacy Officer shall manage compliance issues with Business Associates who use or create and disclose protected health information on the medical practice's behalf.
2. After April 14, 2003, Business Associates shall not be allowed to create, use or disclose protected health information on Physician Practice's behalf without a written agreement retained in the Privacy Record retention system.
3. The Business Associate Agreement shall include the following documented components.
 - Assurance that the Business Associate is in compliance with the general and administrative standards of the Privacy Rule (45 CFR 164.530) and has established reasonable safeguards and minimum necessary standards to limit the incidental use and disclosure of otherwise protected health information.
 - Specific definition of permitted and required uses of the protected information.
 - Assurance that the Business Associates will make available its internal practices, books and records relating to the use and disclosure of protected health information received from, or created by the Business Associate on behalf of Physician Practice to the Privacy Officer or his/her appointee or to the Secretary of HHS for the purposes of determining compliance with assurances provided in the Business Associate Agreement.

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

- Assurance that when the business relationship is terminated protection will be provided past the date of the termination to include returning the protected information if feasible, destroying the documents if practical, or extend the protections provided in the agreement and limit further use of the information.
- Authorize termination of the business relationship between the Business Associate and Physician Practice, if Physician Practice determines that the business associate has violated a material term of the Business Associate Agreement.

Effective Date: _____

Physician Practice, Privacy Officer

DOUG SIMPSON, CPA

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

**HIPAA Policy 2030: PERMITTED USES AND DISCLOSURES TO CARRY OUT
TREATMENT AND COLLECT PAYMENT**

REGULATION: 45 CFR 164.502(c) allows health care providers to use and disclose protected health information for

- Its own treatment, payment and or healthcare operations activities.
- The treatment activities of another health care provider.
- The payment activities of another covered entity or health care provider that receives the information.

OBJECTIVE: Members of the workforce shall have access to the amount of information maintained in a designated record set that is required for them to carry out their assigned duties and responsibilities, but shall always exercise professional caution to limit actual access to the minimum standard required to satisfactorily complete specific assignments, particularly when transmitting information with external parties, or when working with protected information in an area trafficked by individuals who do not need access to the information to complete their job assignments, or trafficked by other patients or the general public.

PROCEDURES:

1. The Privacy Officer shall work with members of the workforce to document the types of medical and billing information that is required for each job function to complete its assigned duties and responsibilities.
2. Members of the workforce shall restrict their access to the medical and billing information required for them to complete their job function.
3. When completing a job function, members of the workforce shall limit the amount of information they use, disclose or receive to the minimum standard that can be reasonably justified to complete their specific job assignment.
4. When access to the medical management information system is required to complete a job function, access to the system shall be restricted by password, and staff trained to complete the function shall complete tasks.
5. Policies in the remainder of this HIPAA Policy Section 2000 are guidelines for the types of medical and billing information that can be accessed by job function, and the conditions that shall normally be met to actually use, disclose, or receive the accessed information

Effective Date: _____

Physician Practice, Privacy Officer

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 2035: PATIENT SCHEDULING JOB FUNCTIONS

REGULATION: 45 CFR 164.502(b)(1) allows for the incidental use or disclosure of otherwise protected health information if the organization has made reasonable efforts to limit the amount of protected health information to the minimum standard required to accomplish the intended purpose of the use, disclosure, or request.

OBJECTIVE: Members of the workforce who perform the patient appointment scheduling job function shall have access to the amount of information maintained in a designated record set that is required for them to carry out their assigned duties and responsibilities, but shall always exercise professional caution to limit actual access to the minimum standard required to satisfactorily complete this specific job assignment, particularly when transmitting information with external parties, or when working with protected information in an area trafficked by individuals who do not need access to the information to complete their job assignments, or trafficked by other patients or the general public.

PROCEDURES:

1. Listed below is a summary of the types of protected health information that may be accessed while completing the Patient Scheduling Job Function:
 - Daily Schedules
 - Patient Demographics
 - Insurance
 - Referring Physician
 - Chief Complaint
 - Account Balance and Payment Status

2. Listed below is a summary of the conditions which shall be followed when accessing these types of protected health information:
 - 2.1. Before contacting an established patient, verify that confidential instructions have not been created for this existing patient. Confidential instructions should be maintained in special instruction data fields maintained in the medical management information system. When confidential instructions have been established, follow the instructions when contacting the patient for scheduling purposes.
 - 2.2. Good judgment shall be used when scheduling patient appointments in person or over the phone, with reasonable precautions taken to segregate this function from the general public or other patients.
 - 2.3. Staff may leave messages on answering machines when patients or other health care providers or health plans are not available to receive phone calls regarding

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

- scheduling information. A message related to appointment notification shall be limited to name, number, and other information necessary to confirm an appointment. A message related to any other medical or business purpose shall be limited to name of the surgical clinic, name of the scheduling staff member, contact number and a request that the individual return the phone call.
- 2.4. Messages may be left with a family member or other person who answers the phone when the patient is not at home. Use professional judgment to assure that such disclosures are in the best interest of the patient, and the message is limited to name of the surgical clinic, name of the scheduling staff member, contact number, and other information necessary to confirm an appointment.
 - 2.5. Appointment schedulers will need access to the medical management information system for the purpose of scheduling a patient visit, for creating or updating demographic and billing information, for verifying open patient responsible account balances, for reviewing daily schedules, for printing copies of schedules, and for preparing encounter forms.
 - 2.6. Appointment schedulers may require access to referring physician records, hospital op reports, laboratory and diagnostic test results, and insurance information. Documents received by facsimile or mail shall be promptly retrieved and placed in the patient chart. When requesting medical records or billing records, limit requests to information requested by the surgeon specifically or by standing order; confirm the transmission address (physical address, telephone number, email address, etc.); confirm the timeframe the request will be fulfilled and when required, follow-up in a timely manner to ensure the information has not been sent to another address.
 - 2.7. Appointment schedulers may communicate patient account balance information to the patient or documented financial guarantor when scheduling follow-up appointments. The purpose of the disclosure shall be to collect the patient responsible balance at the time of the visit or to schedule a meeting with the financial counselor prior to the physician visit.
 - 2.8. Printed schedules are allowed for the purpose of managing physician schedules and managing daily operations. These documents shall be maintained at locations that are not generally accessible to individuals that do not need access to this information.

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

- 2.9. The business office as part of their audit trail shall keep a permanent copy of the daily schedule. Other business functions that use the Daily Schedule as a support document may also retain a copy of the daily schedule in a secure record retention area. All other printed daily schedules should be destroyed at the end of each business day.

_____ **Effective Date:** _____

Physician Practice, Privacy Officer

DOUG SIMPSON, CPA

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 2040: INSURANCE VERIFICATION, REFERRAL CERTIFICATION AND AUTHORIZATION JOB FUNCTIONS

REGULATION: 45 CFR 164.502(b)(1) allows for the incidental use or disclosure of otherwise protected health information if the organization has made reasonable efforts to limit the amount of protected health information to the minimum standard required to accomplish the intended purpose of the use, disclosure, or request.

OBJECTIVE: Members of the workforce responsible for insurance verification, referral certification and authorization job functions shall have access to the amount of information maintained in a designated record set that is required for them to carry out their assigned duties and responsibilities, but shall always exercise professional caution to limit actual access to the minimum standard required to satisfactorily complete specific assignments, particularly when transmitting information with external parties, or when working with protected information in an area trafficked by individuals who do not need access to the information to complete their job assignments, or trafficked by other patients or the general public.

PROCEDURES:

1. Listed below is a summary of the types of protected health information that may be accessed while completing the Insurance Verification, Referral Certification and Authorization Job Function:
 - Daily Schedules
 - Patient Demographics
 - Insurance
 - Assignment of Benefits (AOB)
 - Referring Physician
 - Physician Orders and/or Physician Notes
 - Patient Chart
 - Co-Pay, Financial Status, and AOB Log
2. Listed below is a summary of the conditions which shall be followed when accessing these types of protected health information:
 - 2.1 This job function shall be completed in a supervised work area, with restricted access to the general public. Individually identifiable health information shall not be left unattended. The documents used to complete this function shall be covered when completing other job assignments, shall be stored in a secure environment when the area is unattended, and permanent records shall be

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

promptly returned to the billing office work area or the medical records work area when the job function is completed.

- 2.2 Access to control documents is required to initiate this job function. Examples of control documents include
 - daily schedules,
 - insurance information presented during the scheduling process,
 - insurance card information presented at time of visit, or
 - documentation presented by physician for emergency services provided at another health care facility.
- 2.3 Access to the medical management information system is required to obtain patient demographic and insurance information, and to document verification, referral certification and authorization information required for claims processing and adjudication.
- 2.4 Access to elements of health plans, referring physicians, and other health care facility data record sets may be required to establish accurate billing information.
- 2.5 Access to the medical record may be required obtain a copy of the insurance card and/or the Assignment of Benefits.
- 2.6 Access to the medical record may also be required to review physician orders for procedures or tests requiring authorization.
- 2.7 Before contacting an established patient to obtain billing information, verify that confidential instructions have not been created for this existing patient. Confidential instructions should be maintained in special instruction data fields maintained in the medical management information system. When confidential instructions have been established, follow the instructions when contacting the patient.
- 2.8 Staff may leave messages on answering machines when patients or other health care providers or health plans are not available to receive phone calls regarding billing information. The message shall be limited to name of the surgical clinic, name of the staff member, contact number and a request that the individual return the phone call.
- 2.9 Documents received by facsimile or mail shall be promptly retrieved and may be used to create or update medical management information system data records, then shall be promptly placed in the patient chart. When requesting medical records or billing records, limit requests to information required to complete this job function; confirm the transmission address (physical address, telephone number, email address, etc.); confirm the timeframe the request will be fulfilled and when required, follow-up in a timely manner to ensure the information has not been sent to another address.
- 2.10 The Co-Pay, Financial Status and (AOB) Log shall be created within this function and shall be attached to the Daily Schedule when provided to the Patient Registration Function. The Log shall be stored in a secure location prior to use,

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

and a permanent copy of the Log shall be kept by the business office as part of their audit trail.

_____ **Effective Date:** _____

Physician Practice, Privacy Officer

DOUG SIMPSON, CPA

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 2045: PATIENT REGISTRATION JOB FUNCTIONS

REGULATION: 45 CFR 164.502(b)(1) allows for the incidental use or disclosure of otherwise protected health information if the organization has made reasonable efforts to limit the amount of protected health information to the minimum standard required to accomplish the intended purpose of the use, disclosure, or request.

OBJECTIVE: Members of the workforce shall have access to the amount of information maintained in a designated record set that is required for them to carry out their assigned duties and responsibilities, but shall always exercise professional caution to limit actual access to the minimum standard required to satisfactorily complete specific assignments, particularly when working with protected information in an area trafficked by individuals who do not need access to the information to complete their job assignments, or trafficked by other patients or the general public.

PROCEDURES:

1. Listed below is a summary of the types of protected health information that may be accessed while completing the Patient Registration Job Function:
 - Daily Schedule
 - Patient Demographics
 - Insurance
 - Assignment of Benefits (AOB)
 - Financial Status
 - Patient Encounter Form
 - Patient Sign-In Log
 - Co-Pay, Financial Status, and AOB Log
 - Patient Chart
 - Privacy complaint
 - Confidential instruction
 - Request to inspect or copy medical record or billing record
 - Request to amend medical record or billing record
 - Request to receive an accounting of disclosures
2. Listed below is a summary of the conditions which shall be followed when accessing these types of protected health information:
 - 2.1 In addition to regularly assigned duties, the patient registration desk shall serve as a contact point for handling
 - privacy complaints (see HIPAA Policy 1500 – 1520) for specific privacy job assignments),

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

- requests of confidential treatment of patient information (see HIPAA Policy 4100 for specific privacy job assignments),
 - requests to inspect or make copies of their medical and billing records (see HIPAA Policy 4210 for specific privacy job assignments),
 - requests to amend medical records or billing records (see HIPAA Policy 4300 for specific privacy job assignments), and
 - requests for accounting of disclosures of patient health information (see HIPAA Policy 4400 for specific privacy job assignments).
- 2.2 Good judgment shall always be used and safeguards followed when communicating with individuals during the patient registration process to limit other patients or other persons from indirectly accessing an individual's protected health information.
- 2.3 A patient sign-in sheet may be maintained at the front desk which identifies a patient's name, and patients may be announced by name in the waiting room. However, when handling other individually identifiable information, reasonable precautions shall be taken to segregate this function from the general public or other patients. For example, medical and billing records shall be stored outside the public's view; staff shall only use the volume required to effectively communicate with individuals; and when other individuals are standing at the patient registration area, they shall be asked to step back to afford the level of privacy required to complete the patient registration process.
- 2.4 Each business day, the Daily Schedule, the Co-Pay, Financial Status, and AOB Log, Patient Encounter Forms, and Patient Charts required to accomplish that day's business shall be present in the Patient Registration work area. As such, the work area shall be supervised and these documents shall be protected from unauthorized use or disclosure.
- 2.5 Staff shall access medical management information system modules to the level required to complete the patient registration process.
- 2.6 Staff completing the patient registration function may open patient charts to access insurance cards, driver licenses, assignment of benefit sheets, or other demographic information that may be stored or need to be stored in patient charts.
- 2.7 In an effort to prevent erroneous patient contacts and to prevent erroneous transmission of protected health information, patient contact information (mailing address, telephone number, email address, etc.) and insurance information provided at the time of registration will be matched to demographic and insurance information maintained in the medical management information system when completing the patient registration job function.
- 2.8 Individually identifiable health information shall not be left unattended. The documents used to complete this function shall be covered when completing other job assignments, shall be stored in a secure environment when the area is unattended, and permanent records shall be promptly returned to the billing

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

office work area or the medical records work area when the job function is completed.

_____ **Effective Date:** _____

Physician Practice, Privacy Officer

DOUG SIMPSON, CPA

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

**HIPAA Policy 2050: COLLECTION OF CO-PAYMENT AND DEDUCTIBLE
JOB FUNCTIONS**

REGULATION: 45 CFR 164.502(b)(1) allows for the incidental use or disclosure of otherwise protected health information if the organization has made reasonable efforts to limit the amount of protected health information to the minimum standard required to accomplish the intended purpose of the use, disclosure, or request.

OBJECTIVE: Members of the workforce shall have access to the amount of information maintained in a designated record set that is required for them to carry out their assigned duties and responsibilities, but shall always exercise professional caution to limit actual access to the minimum standard required to satisfactorily complete specific assignments, particularly when working with protected information in an area trafficked by individuals who do not need access to the information to complete their job assignments, or trafficked by other patients or the general public.

PROCEDURES:

1. Listed below is a summary of the types of protected health information that may be accessed while completing the Collection of Co-Payment and Deductible Job Function:
 - Co-Pay, Financial Status, and AOB Log and Patient Encounter Form.
2. Listed below is a summary of the conditions which shall be followed when accessing these types of protected health information:
 - 2.1 Co-payments and deductibles shall be collected as part of the Patient Registration function.
 - 2.2 Detailed information required to complete this job function should be accessed and used as part of the Insurance Verification process, and should be recorded on the Co-Pay, Financial Status, and AOB Log (The Log).
 - 2.3 Access to The Log and the Patient Encounter Form shall be required to complete this job function. The Log shall identify the patient, the insurance plan, and the amount to be collected at the time of service (e.g., co-pay, deductible and financial balance outstanding).
 - 2.4 The amount collected shall be recorded on the Patient Encounter Form.

Effective Date: _____

Physician Practice, Privacy Officer

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

DOUG SIMPSON, CPA

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 2060: FINANCIAL COUNSELING JOB FUNCTIONS

REGULATION: 45 CFR 164.502(b)(1) allows for the incidental use or disclosure of otherwise protected health information if the organization has made reasonable efforts to limit the amount of protected health information to the minimum standard required to accomplish the intended purpose of the use, disclosure, or request.

OBJECTIVE: Members of the workforce shall have access to the amount of information maintained in a designated record set that is required for them to carry out their assigned duties and responsibilities, but shall always exercise professional caution to limit actual access to the minimum standard required to satisfactorily complete specific assignments, particularly when transmitting information with external parties, or when working with protected information in an area trafficked by individuals who do not need access to the information to complete their job assignments, or trafficked by other patients or the general public.

PROCEDURES:

1. Listed below is a summary of the types of protected health information that may be accessed while completing the Financial Counseling Job Function:
 - Billing Report
 - Co-Pay, Financial Status, and AOB Log
 - Demographic
 - Insurance
 - Billing Records
 - Procedure Codes and Diagnosis Codes.
2. Listed below is a summary of the conditions which shall be followed when accessing these types of protected health information:
 - 2.1 The Financial Counseling function may require access to private medical information, billing information, and personal financial information. Therefore, this work product shall be completed in a work area that affords a good level of privacy to openly access and discuss individually identifiable health and financial information.
 - 2.2 Staff shall access medical record documents and billing record documents for the purpose of obtaining copies of relevant information. They may also access the medical management information system to create, update or obtain patient information needed to collect self-responsible balances for professional services rendered.

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

- 2.3 Staff shall not communicate with outside agencies or other charity type organizations on behalf of an individual without the express written authorization of the individual.
- 2.4 Staff may communicate with consumer reporting agencies the following information:

Name and address;
Date of birth;
Social security number;
Payment history;
Account number; and
Name and address of the health care provider and/or health plan.

- 2.5 Working files shall be maintained in a secure record storage area.

Effective Date: _____

Physician Practice, Privacy Officer

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 2070: PATIENT ENCOUNTER JOB FUNCTIONS

REGULATION: 45 CFR 164.502(b)(1) allows for the incidental use or disclosure of otherwise protected health information if the organization has made reasonable efforts to limit the amount of protected health information to the minimum standard required to accomplish the intended purpose of the use, disclosure, or request.

OBJECTIVE: Members of the workforce shall have access to the amount of information maintained in a designated record set that is required for them to carry out their assigned duties and responsibilities, but shall always exercise professional caution to limit actual access to the minimum standard required to satisfactorily complete specific assignments, particularly when transmitting information with external parties, or when working with protected information in an area trafficked by individuals who do not need access to the information to complete their job assignments, or trafficked by other patients or the general public.

PROCEDURES:

1. Listed below is a summary of the types of protected health information that may be accessed while completing Patient Encounter Job Functions:
 - Daily Schedule
 - Patient Encounter Form
 - History and Physical
 - Evaluation and Management
 - Physician Orders, Physician Notes, Op Reports, Dictation
 - Other Health Care Providers
 - Lab Tests and Diagnostic Tests
 - Prescription
2. Listed below is a summary of the conditions which shall be followed when accessing these types of protected health information:
 - 2.1 Direct patient encounters with the nursing and clinical staff shall be completed by trained professionals in a supervised work area, with restricted access to the general public. Individually identifiable health medical documents shall not be left unattended. The documents used to complete this function shall be covered when completing other job assignments, shall be stored in a secure environment when the area is unattended, and permanent records shall be promptly returned to the medical records work area when the job is completed.
 - 2.2 Under the supervision of the physician, the nursing staff and clinical staff shall access, use and disclose the level of medical information required to provide direct quality patient care in an efficient practice environment.

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

- 2.3 Good judgment shall always be used and safeguards followed (see HIPAA policy 1400) when communicating with the patient or with the medical staff to prevent other patients or other persons from indirectly accessing this information in the patient care work areas.
- 2.4 Access to the Daily Schedule, the Pre-Numbered Patient Encounter Forms, the medical record contained in Patient Charts, and the Physician Orders may be required to complete this job function.
- 2.5 Access to the Daily Schedule is required to pull charts and manage patient flow.
- 2.6 Access to pre-numbered patient encounter forms is required to document date of service, diagnosis codes, evaluation and management codes, procedure/diagnostic testing codes associated with the patient visit, and physician signatures.
- 2.7 Access to patient charts is required to obtain and follow instructions required by physician orders, to document history and physical information, to document other medical or clinical services provided during a patient encounter, or to store medical information received from other health care providers.
- 2.8 Prior to a scheduled patient visit, the medical record will be reviewed by a medical person to ensure all orders have been followed, required correspondence and dictation is present, and the data record set is complete.
- 2.9 Individuals shall be escorted from the waiting area to the patient care areas by a member of the medical or clinical staff. When the patient is delivered to their specified area, the patient chart and pre-numbered patient encounter form may be stored outside the exam room. The patient chart shall be placed with patient identification information facing the wall.
- 2.10 When the patient encounter is completed, the patient chart shall either be secured by the physician or shall be returned to the physician's medical record storage area by the medical or clinical person completing the patient encounter; physician orders or instructions and the pre-numbered patient encounter form shall be distributed to the medical or business office staff for processing; and prescription information shall be provided to the patient.
- 2.11 When the physician has completed dictation, the patient chart shall be returned to the medical records work area for storage.
- 2.12 When the physician order or instructions activities have been completed, the documents shall be delivered to the medical records work area for retention in the patient chart.

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

2.13 When the patient encounter is completed, a member of the medical or clinical staff shall ensure that the pre-numbered patient encounter form is completed, and will present the individual, the individual's pre-numbered patient encounter form, and follow-up instructions to the patient check-out area.

Effective Date: _____

Physician Practice, Privacy Officer

DOUG SIMPSON, CPA

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 2080: TRANSMITTING MEDICAL CORRESPONDENCE FOR PATIENT CARE PURPOSES JOB FUNCTIONS

REGULATION: 45 CFR 164.502(b)(1) allows for the incidental use or disclosure of otherwise protected health information if the organization has made reasonable efforts to limit the amount of protected health information to the minimum standard required to accomplish the intended purpose of the use, disclosure, or request.

OBJECTIVE: Members of the workforce shall have access to the amount of information maintained in a designated record set that is required for them to carry out their assigned duties and responsibilities, but shall always exercise professional caution to limit actual access to the minimum standard required to satisfactorily complete specific assignments, particularly when transmitting information with external parties, or when working with protected information in an area trafficked by individuals who do not need access to the information to complete their job assignments, or trafficked by other patients or the general public.

PROCEDURES:

1. Listed below is a summary of the types of protected health information that may be accessed while Transmitting Medical Correspondence for Patient Care Purposes Job Functions:
 - Patient Demographics
 - Other Health Care Providers
 - Physician Orders, Physician Notes, Op Reports, Dictation
 - Lab Tests and Diagnostic Tests
 - Prescription
 - Patient Chart.
2. Listed below is a summary of the conditions which shall be followed when accessing these types of protected health information:
 - 2.1 Medical records may be transmitted to another health care provider by phone, by mail, by facsimile or by electronics.
 - 2.2 Medical correspondence may also be communicated directly to a patient by telephone or by mail using the contact information provided by the patient.
 - 2.3 When requesting medical records or billing records, limit requests to information requested by the physician; confirm the transmission address (physical address, telephone number, email address, etc.); confirm the timeframe the request will be fulfilled and when required, follow-up in a timely manner to ensure the information has not been sent to another address.

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

- 2.4 When sending medical correspondence, the patient chart may be accessed. Document the name of the person requesting the information, the authority they have to obtain the information, the specific information they are requesting, and the transmission address they want used to receive the information, and confirm the timeframe the request will be fulfilled. If there are any questions regarding the propriety of the request (authority to use the information, or the type of information and amount of information requested), consult with a physician before completing the transmission. When the transmission is completed, place the document used to validate the propriety of the request and the fax cover sheet in the patient's privacy file and promptly return the medical information to the patient chart for storage in the medical record work area.
- 2.5 When scheduling lab or diagnostic tests, surgical procedures, and other health care facility admissions, staff shall access demographic and insurance information maintained in the medical management information system, and written orders or instructions provided by the attending physician. Staff shall only disclose the health information required to complete the scheduling process.
- 2.6 Reasonable precautions should be taken to segregate this job function from the general public by practicing good judgment to limit others from overhearing medical conversations or observing other patients medical records. Medical records shall not be left unattended. The documents used to complete this function shall be covered when completing other job assignments, shall be stored in a secure environment when the area is unattended, and permanent records shall be promptly delivered to the medical records work area when the job function is completed.
- 2.7 The facsimile machine shall be maintained in a patient restricted area. When medical correspondence is received, it shall be covered and delivered in a timely manner.
- 2.8 The mail (paper or electronic) shall be sorted and maintained in a patient restricted area. When medical correspondence is received, it shall be promptly distributed in a timely manner.

Effective Date: _____

Physician Practice, Privacy Officer

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 2090: PATIENT CHECK-OUT JOB FUNCTIONS

REGULATION: 45 CFR 164.502(b)(1) allows for the incidental use or disclosure of otherwise protected health information if the organization has made reasonable efforts to limit the amount of protected health information to the minimum standard required to accomplish the intended purpose of the use, disclosure, or request.

OBJECTIVE: Members of the workforce shall have access to the amount of information maintained in a designated record set that is required for them to carry out their assigned duties and responsibilities, but shall always exercise professional caution to limit actual access to the minimum standard required to satisfactorily complete specific assignments, particularly when working with protected information in an area trafficked by individuals who do not need access to the information to complete their job assignments, or trafficked by other patients or the general public.

PROCEDURES:

1. Listed below is a summary of the types of protected health information that may be accessed when completing Patient Check-Out Job Functions:
 - Patient Encounter Form
 - Schedule
2. Listed below is a summary of the conditions which shall be followed when accessing these types of protected health information:
 - 2.1 Good judgment shall always be used and safeguards followed when communicating with individuals during the patient check-out process to limit other patients or other persons from indirectly accessing an individual's protected health information.
 - 2.2 When handling identifiable medical or billing information, reasonable precautions shall be taken to segregate this function from the general public or other patients. For example, medical and billing records shall be stored outside the public's view; staff shall only use the volume required to effectively communicate with individuals; and when other individuals are standing at the patient check-out area, they shall be asked to step back to afford the level of privacy required to complete the patient registration process.
 - 2.3 Patients shall be escorted from the patient care work area to the patient check-out area by a member of the medical staff.
 - 2.4 Staff may access the medical management information system scheduling module to schedule follow-up appointments.
 - 2.5 Staff shall access the pre-numbered patient encounter form to initiate the billing activity sequence. Staff shall validate that the form has been dated, CPT-4 and

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

ICD-9 codes have been designated, and the form has been signed by the attending physician. Staff shall compute and document actual charges and self-responsible balances due to be collected.

- 2.6 Individually identifiable health information used to complete this job function shall not be left unattended. The documents used to complete this function shall be covered when completing other job assignments, shall be stored in a secure environment when the area is unattended, and permanent records shall be promptly delivered to the billing office work area when the job function is completed.

Effective Date: _____

Physician Practice, Privacy Officer

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 2100: “FRONT-END” DAY END PROCESSING JOB FUNCTIONS

REGULATION: 45 CFR 164.502(b)(1) allows for the incidental use or disclosure of otherwise protected health information if the organization has made reasonable efforts to limit the amount of protected health information to the minimum standard required to accomplish the intended purpose of the use, disclosure, or request.

OBJECTIVE: Members of the workforce shall have access to the amount of information maintained in a designated record set that is required for them to carry out their assigned duties and responsibilities, but shall always exercise professional caution to limit actual access to the minimum standard required to satisfactorily complete specific assignments, particularly when working with protected information in an area trafficked by individuals who do not need access to the information to complete their job assignments, or trafficked by other patients or the general public.

PROCEDURES:

1. Listed below is a summary of the types of protected health information that may be accessed when completing the Business Office’s, “Front –End” Day End Processing Job Functions:
 - Daily Schedule
 - Patient Sign-In Register
 - Co-Pay, Financial Status, and AOB Log (Log)
 - Daily Batch Summary Sheet
 - Pre-numbered Patient Encounter Forms
2. Listed below is a summary of the conditions which shall be followed when accessing these types of protected health information:
 - 2.1 “Front –End” Day End Processing activities shall not be completed in work areas trafficked by the general public. Individually identifiable health information used to complete this job function shall not be left unattended. Permanent records shall be promptly delivered to the billing office work area when the job function is completed and patient charts pulled for the next day schedule shall be locked up in a protected environment.
 - 2.2 Access to all the Business Office’s permanent records created during the business day shall be required to complete this job function.
 - 2.3 The Daily Schedule and the Patient Sign-In Register will be matched to individual, pre-numbered patient encounter forms to ensure that a charge ticket has been established for each patient visit.
 - 2.4 The Log and individual, pre-numbered patient encounter forms will be matched to ensure that cash receipts have been properly posted.

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

- 2.5 The Log will be matched to new AOB's to ensure current information is maintained in the billing record.
- 2.6 The Log will be matched to new Insurance Cards to ensure current information is maintained in the billing record.
- 2.7 The Log will be matched to new financial plans and pre-numbered patient encounter forms to ensure that self pay balances have been collected and recorded.
- 2.8 Pre-numbered patient encounter forms will be reviewed to ensure that date of service has been documented, CPT-4 and ICD-9 codes have been identified, charges have been recorded, changes have been initialed by the attending physician, and the document has been signed by the attending physician.
- 2.9 A Daily Batch Summary Sheet (Control Document) shall be completed. The Control Document shall report total charges, report total cash and checks collected (matched to the bank deposit slip), and total credit card receipts collected. The original Daily Schedule, the original Patient Sign-In Register, the original Log, the original pre-numbered, patient encounter forms, a copy of the bank deposit slip, a copy of the front and back of new insurance cards, a copy of the new AOB's, and a copy confidential patient instructions shall be attached to the Daily Batch Summary Sheet.
- 2.10 These permanent records shall be promptly delivered to the billing office work area when the job function is completed.
- 2.11 The "Next Day" Schedule shall be printed. The next day schedule shall be used as the source document for pulling patient charts. Pre-numbered, patient encounter forms shall be printed and attached to the patient chart. These charts and patient encounter forms shall be secured in a protected area in preparation for use during the next day business.

Effective Date: _____

Physician Practice, Privacy Officer

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 2110: POSTING PATIENT CHARGES JOB FUNCTIONS

REGULATION: 45 CFR 164.502(b)(1) allows for the incidental use or disclosure of otherwise protected health information if the organization has made reasonable efforts to limit the amount of protected health information to the minimum standard required to accomplish the intended purpose of the use, disclosure, or request.

OBJECTIVE: Members of the workforce shall have access to the amount of information maintained in a designated record set that is required for them to carry out their assigned duties and responsibilities, but shall always exercise professional caution to limit actual access to the minimum standard required to satisfactorily complete specific assignments, particularly when transmitting information with external parties, or when working with protected information in an area trafficked by individuals who do not need access to the information to complete their job assignments, or trafficked by other patients or the general public.

PROCEDURES:

1. Listed below is a summary of the types of protected health information that may be accessed when completing Charge Posting Job Functions:
 - Daily Schedule
 - Patient Sign-In Register
 - Co-Pay, Financial Status, and AOB Log
 - Daily Batch Summary Sheet
 - Pre-numbered Patient Encounter Forms
 - Patient Demographics
 - Billing
2. Listed below is a summary of the conditions which shall be followed when accessing these types of protected health information:
 - 2.1 Charge posting activities shall not be completed in work areas trafficked by the general public. Individually identifiable health information used to complete this job function shall not be left unattended. The documents used to complete this function shall be covered when completing other job assignments, shall be stored in a secure environment when the area is unattended, and permanent records shall be promptly stored in the billing office's record retention system when the job function is completed.
 - 2.2 Access to the Daily Batch Summary Sheet and its attachments is required to complete this job function and to supervise successful completion of "front-end" business office procedures.

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

- 2.3 Access to the medical management information system charge posting module and balancing reports is also required to complete this job function. When updates or corrections are required to successfully bill an individual patient account, other billing modules and the patient note system may be accessed to complete this job function.

Effective Date: _____

Physician Practice, Privacy Officer

DOUG SIMPSON, CPA

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 2120: BILLING PATIENT CLAIMS JOB FUNCTIONS

REGULATION: 45 CFR 164.502(b)(1) allows for the incidental use or disclosure of otherwise protected health information if the organization has made reasonable efforts to limit the amount of protected health information to the minimum standard required to accomplish the intended purpose of the use, disclosure, or request.

OBJECTIVE: Members of the workforce shall have access to the amount of information maintained in a designated record set that is required for them to carry out their assigned duties and responsibilities, but shall always exercise professional caution to limit actual access to the minimum standard required to satisfactorily complete specific assignments, particularly when transmitting information with external parties, or when working with protected information in an area trafficked by individuals who do not need access to the information to complete their job assignments, or trafficked by other patients or the general public.

PROCEDURES:

1. Listed below is a summary of the types of protected health information that may be accessed when completing Patient Claims Processing Job Functions:
 - Billing
 - Paper Claims
 - Medical data records
 - Patient Chart
2. Listed below is a summary of the conditions which shall be followed when accessing these types of protected health information:
 - 2.1 Claims Processing activities shall not be completed in work areas trafficked by the general public. Individually identifiable health information used to complete this job function shall not be left unattended. The documents used to complete this function shall be covered when completing other job assignments, shall be stored in a secure environment when the area is unattended, and permanent records shall be promptly stored in the billing office's record retention system when the job function is completed.
 - 2.2 The medical management information system health plan/insurance carrier database shall be managed to ensure correct claims submission information is maintained by the Billing Office, and staff shall be trained and supervised to ensure health plan/insurance carrier billing codes are correctly assigned to individual patient account data fields before claims are transmitted for payment.
 - 2.3 Access to the medical management information system billing modules, balancing reports, and edit reports is required to complete this job function.

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

When updates or corrections are required to successfully bill an individual patient account, other billing modules and the patient note system may be accessed to complete this job function.

- 2.4 Certain third party payers require medical documentation to support the claim for reimbursement. Patient charts may be accessed to obtain medical documentation required to support the claims submission process. Patient charts may also be accessed to obtain copies of demographic information, insurance information, and AOB. In all cases, access to the patient chart shall be limited to obtaining billing information, and shall be restricted to the minimum amount of information required to support the claims process or to update demographic and insurance information maintained in the medical management information system database.
- 2.5 Paper claims shall be printed on the Billing Office printer. The Billing Office printer shall be maintained in a patient restricted area and shall only be used for Billing Office purposes. When claims are printed for mailing, procedures shall be completed in a timely manner to ensure prompt delivery to the U.S. postal service.
- 2.6 The Billing Office shall submit electronic claims on a scheduled basis. Edit reports shall be managed and processed in a timely manner. Edit reports and confirmation receipts shall be retained as a permanent record within the Billing Office record retention system.

Effective Date: _____

Physician Practice, Privacy Officer

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 2130: CLAIMS ADJUDICATION JOB FUNCTIONS

REGULATION: 45 CFR 164.502(b)(1) allows for the incidental use or disclosure of otherwise protected health information if the organization has made reasonable efforts to limit the amount of protected health information to the minimum standard required to accomplish the intended purpose of the use, disclosure, or request.

OBJECTIVE: Members of the workforce shall have access to the amount of information maintained in a designated record set that is required for them to carry out their assigned duties and responsibilities, but shall always exercise professional caution to limit actual access to the minimum standard required to satisfactorily complete specific assignments, particularly when transmitting information with external parties, or when working with protected information in an area trafficked by individuals who do not need access to the information to complete their job assignments, or trafficked by other patients or the general public.

PROCEDURES:

1. Listed below is a summary of the types of protected health information that may be accessed when completing Claims Adjudication Job Functions:
 - Billing
 - Paper Claims
 - Medical Record
2. Listed below is a summary of the conditions which shall be followed when accessing these types of protected health information:
 - 2.1 Claims Adjudication activities shall not be completed in work areas trafficked by the general public. Individually identifiable health information used to complete this job function shall not be left unattended. The documents used to complete this function shall be covered when completing other job assignments, shall be stored in a secure environment when the area is unattended, and permanent records shall be promptly stored in the billing office's record retention system when the job function is completed.
 - 2.2 Access to the medical management information system billing modules, billing reports, balancing reports, edit reports and the patient note system may be accessed to complete this job function.
 - 2.3 Access to third party payer and individual payer correspondence may be required to complete this job function.
 - 2.4 Certain third party payers require medical documentation to support the claim for reimbursement. Patient charts may be accessed to obtain medical documentation required to support the claims submission process. Patient charts may also be

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

- accessed to obtain copies of demographic and insurance information. In all cases, access to the patient chart shall be limited to obtaining billing information, and shall be restricted to the minimum amount of information required to support the claims adjudication process.
- 2.5 Billing Correspondence may be transmitted to a health plan/insurance carrier or another health care provider by phone, by mail, by facsimile or by electronics.
 - 2.6 Billing correspondence may also be communicated directly to a patient by telephone or by mail using the contact information provided by the patient.
 - 2.7 When requesting medical record information from another healthcare provider, limit requests to the specific information required to complete the claims adjudication process; confirm the transmission address (physical address, telephone number, email address, etc.); confirm the timeframe the request will be fulfilled and when required, follow-up in a timely manner to ensure the information has not been sent to another address.
 - 2.8 When sending a copy of medical record information or billing record information to a health plan/insurance carrier to complete the claims adjudication process, follow the transmission instructions provided on the correspondence, and limit the disclosure of medical information to the specific information requested by the health plan/insurance carrier representative. When the transmission is completed, place the health plan/insurance carrier correspondence and the fax cover sheet in the patient's privacy file and promptly return the medical information and billing information to the patient chart for storage in the medical record work area.
 - 2.9 The facsimile machine shall be maintained in a patient restricted area. When medical correspondence or billing correspondence is received for claims adjudication purposes, the documentation shall be delivered to the billing office for distribution and use in a timely manner. The Billing Office shall make a copy of the correspondence, and forward it to the medical records work area for storage in the individual's patient chart.

Effective Date: _____

Physician Practice, Privacy Officer

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

**HIPAA Policy 3000: NOTICE OF PRIVACY PRACTICES FOR PROTECTED
HEALTH INFORMATION**

REGULATION: 45 CFR 164.520(a) provides for an individual's right to notification of how a health care provider shall use and disclose their protected health information, and the individual's rights and the health care provider's legal duties with respect to protected health information.

OBJECTIVE: **Physician Practice** shall provide individuals with a written explanation (Notice of Privacy Practices) of how the medical practice shall use and disclose their protected health information, and the members of the workforce shall then abide by the terms of the Notice of Privacy Practices.

PROCEDURES:

1. The Privacy Officer shall establish a Notice of Privacy Practices for protected health information that includes the information required by 45 CFR 164.520(a), and conforms to the example of the Notice of Privacy included at the end of this policy.
2. When material changes are made to Privacy Policies and Procedures, the Privacy Officer shall ensure that the Notice of Privacy Practices is revised to communicate the changes, the revised Notice of Privacy Practices is effectively communicated to patients, and the effective date of the changes in policies and procedures does not occur before the effective date of the revised Notice of Privacy Practices.
3. A copy of the Notice of Privacy Practices shall be prominently displayed in the waiting area.
4. A copy of The Notice of Privacy Practices shall be offered to each new patient when they register for their first office visit along with a cover sheet. The patient shall sign the cover sheet and the cover sheet shall remain as part of the patient's privacy record in the patient's medical record. If the patient refuses to sign the cover sheet, simply note on the document that the Notice of Privacy Practices was offered to the patient, and include the cover sheet in the patient's medical record.
5. A copy of the Notice of Privacy Practices shall be retained as a permanent record for a period of six years from the creation date or its last effective date, whichever is later.

Effective Date: _____

Physician Practice, Privacy Officer

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

**ACKNOWLEDGEMENT OF RECEIPT OF
NOTICE OF PRIVACY PRACTICES**

Physician Practice is committed to protecting your privacy and ensuring that your health information is used and disclosed appropriately. This Notice of Privacy Practices identifies all potential uses and disclosures of your health information and outlines your rights with regard to your health information. Please sign the form below to acknowledge that you have received our Notice of Privacy Practices.

I acknowledge that I have received a copy of the Notice of Privacy Practices of Physician Practice.

Name: _____.

Signature: _____.

Date: _____.

DOUG SIMPSON, CPA

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

**Physician Practice
“Notice of Privacy Practices”**

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

USES AND DISCLOSURES:

Treatment: Your health information may be used by our staff members or disclosed to other health care professionals for the purpose of evaluating your health, diagnosing your medical condition, and providing treatment. For example, medical notes and medical correspondence and results of laboratory tests and diagnostic tests shall be retained in your medical record. This health information shall be made available to other health care professionals who are involved in your health care.

Payment: Your health information may be used to seek payment from your health plan, other sources of coverage (e.g. automobile insurance), credit card companies you may use to pay for your services, financial guarantors, and collection services. For example, your health plan may request and shall receive information on dates of services, the services provided, and the medical condition being provided.

Health care operations: Your health information may be used as necessary to support the day-to-day activities and management of Physician Practice. For example, information on the services you have received may be used for budgeting and financial reporting purposes, and activities to evaluate and promote quality.

Law enforcement: Your health information may be disclosed to law enforcement agencies, judicial and administrative agencies, without your permission to support government audits and inspections, to facilitate law enforcement investigations, and to comply with government mandated reporting.

Public health reporting: Your health information may be reported to public health agencies as required by law. For example, we are required to report certain communicable diseases to the state’s public health department.

Other uses and disclosures require your authorization: Disclosures of your health information or its use for any purpose other than described above requires your specific written authorization. You may change your mind after you have provided us with a written authorization to use or disclose your information for a specific purpose. However, your decision to revoke an authorization will not affect or undo any use or disclosure of information that occurred before you notified us of your decision to revoke the authorization.

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

ADDITIONAL USE OF HEALTH INFORMATION:

Appointment notification: Your health information will be used by our staff to notify you of appointment reminders or to deliver a message that you need to contact the medical office. Please notify staff in writing during the registration process if you have special instructions for receiving communications from us by alternative means or at alternative locations.

Coordination of health care: When we determine it is in your best medical interest, we shall disclose to family members, relatives or close friends that information which we believe is directly relevant to their involvement in your health care. Please notify the physician during your office visit if you object to this use of your protected health information.

INDIVIDUAL RIGHTS:

The right to request certain restrictions on the use and disclosure of protected health information. Please notify your physician if you want to restrict the use or disclosure of certain information we will use to carry out treatment, payment or health care operations. If the physician agrees to the requested restriction of otherwise permitted or required use or disclosure of your protected health information, you will need to describe the restriction in writing. Physician Practice reserves the right to use or disclose restricted information if you require emergency treatment and the information is required for that treatment.

The right to receive confidential communications of protected health information. Please notify staff in writing during the registration process if you have special instructions for handling payment information or for receiving communications from us.

The right to inspect and copy protected health information. If you would like to inspect or make a copy of your medical record, please submit your written request to the patient registration staff. If the information you have requested is maintained in our active recordkeeping system, we will respond to your request within 30 days. If the information has been archived, it may take an additional 30 days to obtain your records and respond to your request. You will be charged a reasonable, cost-based fee for this service. Physician Practice reserves the right to restrict access to all or part of an individual's medical record as required by law.

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

The right to amend protected health information. If you would like your physician to amend the protected health information that is maintained in your medical record, please submit a written request to your physician describing your requested action. Physician Practice will act upon your request within 30 days.

The right to receive an accounting of disclosures of protected health information. Beginning April 14, 2003, we are required to maintain a record of each time we disclose your protected health information for any purpose other than to carry out treatment, payment and health care operations or pursuant to a valid authorization; or for national security, intelligence and correctional institution purposes. If you would like a copy of your disclosure record, please submit your written request to the patient registration staff. Physician Practice will act upon your request within 60 days, and we will provide the first accounting in any 12-month period to you free of charge.

Physician Practice DUTIES:

Physician Practice is required by law to maintain the privacy of your protected health information and to provide you notice of our legal duties and privacy practices with respect to your protected health information. Physician Practice is required to abide by the terms of this notice.

As permitted by law, we reserve the right to revise or change our privacy policies and procedures and the terms of our Notice of Privacy Practices, and to make the new notice provisions effective for all protected health information it maintains. Whenever a revision is made, we will provide you with the revised notice on your next office visit.

COMPLAINTS:

We are very concerned about protecting our patients' privacy rights, and are always interested in your comments and concerns. If you would like to submit a comment or complaint regarding our current privacy practices, we encourage you to do so by sending a letter outlining your concerns to:

**Physician Practice
2911 Medical Art Street #2
Austin, Texas 78705**

If you believe that your privacy rights have been violated, please do not hesitate to call the matter to our attention by sending a letter describing the cause of your concern to the same address. You may also contact the Secretary of the Department of Health and Human Services.

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

CONTACT PERSON:

The name and address of the person you can contact for further information is:

**Street Address
Austin, Texas 78705
Phone Number**

EFFECTIVE DATE:

This Notice is effective on or after April 14, 2003.

DOUG SIMPSON, CPA

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 4000: RIGHTS OF INDIVIDUALS TO REQUEST RESTRICTIONS ON DISCLOSING AND USING PROTECTED HEALTH INFORMATION

REGULATION: 45 CFR 164.522(a)(1) states that a health care provider must permit an individual to request that a health care provider restrict the use and disclosure of protected health information that would otherwise be permitted to be used or disclosed to carry out treatment, payment or health care operations, or to coordinate care or payment with closely identified person's who are directly involved in the individual's health care.

The health care provider is not required to agree with the restriction, but if they do agree to the restriction, they may not violate the restriction unless the individual requires emergency treatment, and the restricted information is required as part of the emergency treatment.

REGULATION: 45 CFR 164.522(a)(2) states that a health care provider may terminate an agreed-upon restriction if the individual requests the termination or if the health care provider informs the individual that it is terminating the restriction. The termination is only effective for information created or received after the effective date of the termination.

OBJECTIVE:

The Notice of Privacy Practices shall inform individuals of their right to request restrictions on certain uses of their health information, and the procedures used to make the request. The medical practice does not have to agree to these requests. Therefore, careful consideration shall be given to agreeing to a restriction.

All agreed-upon restrictions shall be clearly documented by the individual and communicated to the staff.

All members of the workforce shall comply with the terms of the restriction.

PROCEDURES:

1. The Privacy Officer shall establish a Notice of Privacy Practices for protected health information that includes information of an individual's right to request restrictions on their health information (see HIPAA Policy 3000).
2. The physicians are the only members of the workforce who may agree to the terms of restriction requested by an individual.
3. The individuals request must be made in writing, it must clearly define the restriction requested, and it must be signed and dated by the individual (Restriction).

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

4. If the physician agrees to the terms, the physician shall sign and date the document, and shall provide written instructions that clearly define how the staff shall use and disclose the individual's health information (Instructions).
5. A copy of the Restriction and the Instructions shall be retained in the patient chart, and a copy of the documents shall be retained in the permanent record retention system used for privacy documents. The Instructions shall also be documented in a special instructions field of the medical management information system.
6. The restricted information may be used or disclosed if the individual is in need of the emergency treatment, and the information is required to provide the emergency treatment. If the information is disclosed to another health care provider, the physician must request that the other health care provider not further use or disclose the restricted information.
7. When an individual elects to remove the restriction, the election must be clearly documented by the patient or when necessitated, by the physician. Restriction records maintained in the patient chart and the medical management information system special instructions field shall be removed, and all documentation related to the termination agreement shall be placed in the permanent record retention system used for privacy documents.
8. The physician may elect to terminate a restriction. The physician may provide written evidence of such action directly to the individual or may deliver the letter by U.S. Postal Service, certified mail. This termination shall only effect protected health information created or received after the effective date of the physician's letter. A copy of the Termination Letter shall be retained in the patient chart, and a copy of the document shall be retained in the permanent record retention system used for privacy documents. Information maintained in a special instructions field of the medical management information system shall be revised to document the effective date of the termination.

Effective Date: _____

Physician Practice, Privacy Officer

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 4100: RIGHTS OF INDIVIDUALS TO PLACE CONFIDENTIAL COMMUNICATION REQUIREMENTS ON PROTECTED HEALTH INFORMATION

REGULATION: 45 CFR 164.522(b)(1) states that a health care provider must permit an individual to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the health care provider by alternate means or at alternate locations.

The health care provider may condition the provision of reasonable accommodation on information as to how payment is to be handled; and specifications of an alternate address or other method of contact.

OBJECTIVE:

The Notice of Privacy Practices shall inform individuals of their right to request confidential treatment of certain protected health information. Physician Practice shall accommodate reasonable requests to protect sources of payment, and to communicate with the individual at alternate addresses or by alternate methods defined by the individual. For example, at the individual's request, we may use a P.O. Box address instead of the individual's permanent mailing address to submit correspondence; and we may facsimile or telephone information to the individual's work numbers instead of the individual's home telephone numbers when contacting the individual to obtain or communicate information.

Once alternative means or alternative locations have been documented in writing, members of the workforce shall not violate the individual's confidence.

PROCEDURES:

1. The Privacy Officer shall establish a Notice of Privacy Practices for protected health information that includes information of an individual's right to request confidential treatment of payment or contact information (see HIPAA Policy 3000).
2. Patient registration staff members shall handle confidential communication requests. When completing this job function, safeguards shall be strictly followed to protect the individual's privacy, and to prevent the incidental use or disclosure of otherwise protected health information.
3. The Privacy Officer shall resolve questions regarding the practical ability to meet confidentiality requests.
4. Requests for confidential treatment of payment information or contact information (Request for Confidentiality) shall be submitted in writing, shall be signed and dated by the individual, and shall provide specific instruction on what information is to be

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

handled in a confidential manner, and what alternate methods or locations the medical practice shall use to communicate with the individual.

5. A copy of the Request for Confidentiality shall be retained in the patient chart, a copy shall be forwarded to the billing office, and a copy shall be retained in the permanent record retention system used for privacy documents.
6. Alternate information shall be documented as primary information in applicable fields used to document individual and third party contact information in the medical management information system. Special instruction fields shall be used to note that the individual has requested confidential treatment of specific information, and shall document specific instructions provided by the individual to handle this confidential information.
7. The Billing Office shall verify that information included on the Request for Confidentiality matches the information maintained in the medical management information system.
8. Members of the workforce shall follow administrative procedures required to identify when alternate methods and addresses are required to communicate with an individual, and they shall use those alternative methods or addresses to complete their job assignments.

Effective Date: _____

Physician Practice, Privacy Officer

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 4200: DESIGNATED RECORD SETS SUBJECT TO ACCESS BY INDIVIDUALS

REGULATION: 45 CFR 164.524(e)(1) states that a health care provider must document the designated record sets that are subject to access by individuals.

REGULATION: 45 CFR 164.501 defines a designated record set as medical records and billing records about individuals maintained by or for a health care provider.

OBJECTIVES:

Physician Practice shall maintain an individual record retention system for medical records and billing records. Patient health information shall be stored in readily identifiable record sets. The designated record sets may be stored at the medical office location, or archived off-site in a secure environment. Designated record sets can be maintained in hard copy or electronic format.

A designated record set shall include information about an individual that is used in whole or in part by or for Physician Practice to make medical or payment decisions about the individual. The information shall be maintained at least 6 years from the date of creation.

PROCEDURES:

1. A designated record set shall be established for each patient.
2. Information included in the designated record set shall be maintained in the patient chart and in the medical management information system. Listed below is a summary of documents maintained in the patient chart:
 - Original and revised demographic and financial information provided by the individual or the individual's financial guarantor.
 - Information about an individual that is used in whole or in part by or for Physician Practice to make medical decisions about the individual.
 - Agreed-upon restrictions to use or disclosure of protected information.
 - Confidentiality instructions established with the individual.
3. Billing information shall be maintained in electronic format in the medical management information system in required data fields and in the note system. Access to the medical management information system shall be restricted by password. A back up of information maintained in the medical management information system database shall be completed each day. The back-up records may be stored on-site in a fireproof environment that is only accessible to designated key

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

employees, or it may be stored at a business associates location subject to a Business Associate Agreement (see HIPAA policy 2025.)

4. An individual has the right to inspect or copy the information maintained in their designated record set in accordance with HIPAA Policy 4210.

Effective Date: _____

Physician Practice, Privacy Officer

DOUG SIMPSON, CPA

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 4210: RIGHTS OF INDIVIDUALS TO INSPECT AND COPY THEIR PROTECTED HEALTH INFORMATION

REGULATION: 45 CFR 164.524(a)(1) states that an individual has a right of access to inspect and obtain a copy of their protected health for as long as the protected health information is maintained by the health care provider in a designated record set.

Unreviewable grounds for denial (45 CFR 164.524(a)(2). A health care provider may deny an individual access without providing the individual an opportunity for review in the following circumstances:

- When information has been compiled in reasonable anticipation of or for use in civil, criminal, or administrative action proceedings.
- When the health care provider is acting under the direction of a correctional institution, the health care provider can deny inmates' access to their records if the health care provider believes that the requested access would jeopardize the health, safety, security, etc. of the inmate or those around them.
- If the information was obtained by someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

Reviewable grounds for denial (45 CFR 164.524(a)(3). A health care provider may deny individual access, provided that the individual is given a right to have such access reviewed,

- When the health care provider believes in their exercise of professional judgment access to the information would endanger the life or physical safety of the individual or another person, or would likely cause substantial harm to the individual or other persons (unless the other person is a health care provider).
- When the request is made by a personal representative and the health care provider believes in their exercise of professional judgment that the provision of access to the personal representative would likely cause substantial harm to the individual or to others.

Review of a denial of access (45 CFR 164.524(a)(4). When an individual requests that their denial be reviewed, the health care provider must promptly submit the individual's request for review to a licensed health care professional who was not directly involved in the decision to deny the individual access to their protected health information. The designated reviewing official must then, within a reasonable time period, determine whether access to the protected health information shall be allowed or denied based on the standards outlined above.

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

The health care provider shall promptly provide written notice to the individual when a determination has been made, and shall take other action as required to carry out the designated reviewing official's determination.

OBJECTIVE:

The Notice of Privacy Practices shall inform individuals of their right to inspect and copy their protected health information. Physician Practice shall provide access or deny access to individuals based on the guidelines described above, and the procedures set forth below:

PROCEDURES:

1. The Privacy Officer shall establish a Notice of Privacy Practices for protected health information that includes information of an individual's right to inspect and copy their protected health information (see HIPAA Policy 3000).
2. Requests to inspect or copy medical records must be submitted in writing by the individual.
3. A \$25 fee will be charged for this service. The fee shall be collected before the service is initiated.
4. The patient registration staff shall serve as the contact person for handling these requests. When completing this job function, safeguards shall be strictly followed to protect the individual's privacy, and to prevent the incidental use or disclosure of otherwise protected health information.
5. The physician shall review the request and the medical record, and identify those records which shall be made available to the individual (in whole or in part) based on the standards defined in this policy and further defined in 45 CFR 164.524(a)(1-3).
6. Physician Practice has 30 days to respond to the individual's request. Responses may include
 - Providing access as requested.
 - Providing a letter informing the individual that the records are maintained off-site and an additional 30 days may be required to obtain the records.
 - Providing a letter stating that the requested information is no longer available because the dates of service for the requested information exceed our record retention policy of maintaining designated record sets for six years. If the physician knows another location that the medical information is maintained, the letter must disclose this information. If the physician does not know of an alternate source, the letter may include suggestions of other sources (e.g., admitting hospital, referring physician) of access for the individual.
 - Providing a letter denying access (in whole or in part). The letter must include the following elements:

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

- 1) The basis for the denial.
 - 2) A statement of the individual's right to review (if applicable), with instructions on how to contact the Privacy Officer to exercise such rights.
 - 3) A statement of the individual's right to complain as defined in the Notice of Privacy Procedures or directly to the Secretary of Health and Human Services.
7. All written documents (e.g., individual's written request, physician correspondence, and copy of medical records provided to individual) shall be retained in the permanent record retention system used for privacy documents.

Effective Date: _____

Physician Practice, Privacy Officer

DOUG SIMPSON, CPA

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

HIPAA Policy 4220: DENIAL OF ACCESS REVIEW PROCESS

REGULATION: 45 CFR 164.524(a)(4) provides for an individual's right to request a review of a health care providers decision to deny the individual access to information maintained in a designated record set. When an individual requests that their denial be reviewed, the health care provider must promptly submit the individual's request for review to a licensed health care professional who was not directly involved in the decision to deny the individual access to their protected health information. The designated reviewing official must then, within a reasonable time period, determine whether access to the protected health information shall be allowed or denied based on the standards outlined above. The health care provider shall promptly provide written notice to the individual when a determination has been made, and shall take other action as required to carry out the designated reviewing official's determination.

OBJECTIVE:

When access is denied by a physician and the individual has a right to request a review of that decision, and does request a review in writing, Physician Practice shall comply with the request in accordance with the specifications outlined in 45 CFR 164.524(a)(4).

PROCEDURES:

1. The Privacy Officer shall be responsible for coordinating the review process with a licensed health care professional who is independent of the original decision to deny access to the medical record.
2. The request for review should specify a completion date, and the Privacy Officer shall track the referral to timely completion.
3. The health care provider shall promptly provide written notice to the individual when a determination has been made, and shall take other action as required to carry out the designated reviewing official's determination.
4. All correspondence pertaining to the review process shall be retained in the permanent record retention system used for privacy documents.

Effective Date: _____

Physician Practice, Privacy Officer

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 4300: RIGHT TO AMEND PROTECTED HEALTH INFORMATION

REGULATION: 45 CFR 164.526(a) provides for an individual's right to have a health care provider amend protected health information or a specific record maintained in their designated record set. Listed below are conditions by which a health care provider may deny the individual's request:

- The information or the record is accurate and complete.
- The information requested to be amended is not part of the designated record set maintained by the health care provider.
- The information or the record was not created by the health care provider unless the individual provides a reasonable basis to believe that the originator of the protected health information is no longer available to act on the requested amendment.

OBJECTIVE:

The Notice of Privacy Practices shall inform individuals of their right to amend protected health information maintained in their designated record set. Physician Practice shall either amend requested information or records or shall deny the requested amendment based on the conditions described above, and the procedures set forth below:

PROCEDURES:

1. The Privacy Officer shall establish a Notice of Privacy Practices for protected health information that includes information of an individual's right to amend protected health information maintained in their designated record set (see HIPAA Policy 3000).
2. Amendment requests must be submitted in writing by the individual and must provide a reason to support a requested amendment.
3. The patient registration staff shall serve as the contact person for handling these requests. When completing this job function, safeguards shall be strictly followed to protect the individual's privacy, and to prevent the incidental use or disclosure of otherwise protected health information.
4. Physician Practice must act on the individual's request within 60 days of receipt of the request. A one-time 30-day extension is available if the physician provides written notice of the cause of the delay and the date that the action will be completed.
5. The physician shall review the request and the medical record, and shall determine whether to grant or deny the request for amendment in whole or in part

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

based on the conditions defined in this policy and further defined in 45 CFR 164.526(a)(2)(i.-iv.).

6. If the physician accepts the requested amendment in whole or in part, the following requirements must be met:
 - At a minimum, identify the records in the designated record set that are affected by the amendment and append the amendment to those records.
 - Promptly notify the individual in writing that the amendment has been accepted; request written permission to share the amended information with relevant individuals to whom the amended information needs to be shared, and request a list of people the individual knows that needs access to the amended information. The individual will need to provide written authorization for Physician Practice to disclose the amended information.
 - Make a reasonable effort in a reasonable time to inform and provide the amended information to the people who are identified by the individual to receive the information, as well as other people the physician knows may have relied upon or could foreseeably rely upon the original information to the detriment of the individual.

7. If the physician denies the requested amendment in whole or in part, the following requirements must be met:
 - 7.1 Timely, written denial (45 CFR 164.526(d)(1)(i.-iv.)): The physician must provide a written denial to the individual. The letter must be written in plain language and contain the following elements:
 - Disclose the basis for the denial as outlined in this policy.
 - A statement of the individual’s rights to submit a written statement disagreeing with the denial and providing the individual the Privacy Officer’s contact information should they choose to file a statement of disagreement.
 - Include the following statement,

If you do not submit a statement of disagreement, you may request that Physician Practice provide your request for amendment and our denial of your request with any future disclosure of the protected health information that is the subject of the amendment.
 - A statement of the individual’s right to complain as defined in the Notice of Privacy Procedures or directly to the Secretary of Health and Human Services.

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

- 7.2 Statement of disagreement (45 CFR 164.526(d)(2)): The individual's statement of denial must be incorporated into the individual's medical record as described in the recordkeeping section of this procedure.
 - 7.3 Statement of rebuttal (45 CFR 164.526(d)(3)): The physician may elect at their discretion to prepare a rebuttal statement to the individual's statement of disagreement. The physician's rebuttal statement must be incorporated into the individual's medical record as described in the recordkeeping section of this procedure. A copy of the rebuttal statement must be submitted to the individual who submitted the statement of disagreement.
 - 7.4 Recordkeeping (45 CFR 164.526(d)(4)): The physician must identify the information in the individual's designated record set that is in question and must append or otherwise link the request for amendment, the physician's written denial, the statement of disagreement (if applicable), and the statement of rebuttal (if applicable) to the designated record set.
 - 7.5 Future disclosures (45 CFR 164.526(d)(5)): Future disclosures of the information subject to the disagreement must include documents appended or linked to the information in dispute.
8. A copy of all correspondence pertaining to either granting or denying the request to amend an individual's protected health information shall be retained in the permanent record retention system used for privacy documents.

Effective Date: _____

Physician Practice, Privacy Officer

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

HIPAA Policy 4400: RIGHT TO AN ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

REGULATION: 45 CFR 164.528(a) requires a health care provider to maintain a record of each time they disclose an individual's protected health information for any purpose other than to carry out treatment, payment and health care operations or pursuant to a valid authorization; or for national security, intelligence and correctional institution purposes. The accounting period shall begin with disclosures made on April 14, 2003.

OBJECTIVE:

Physician Practice shall maintain a permanent record retention system used for privacy documents. Records shall be maintained in individually identifiable record sets. Listed below is a summary of disclosures made by Physician Practice or a business associate that must be included in a patient's designated privacy record set to support an accounting to individuals:

- **Disclosure of information requiring an individual's authorization when an authorization was not obtained as instructed by legal counsel.**
- **Victims of abuse, neglect or domestic violence (This section does not apply to suspected victims of child abuse or neglect.)** A copy of patient health information disclosed to government authorities who are authorized to receive reports of domestic violence, abuse and neglect, as well as the following support document:

Written authorization from the victim or patient representative to release information. If the patient is unable to agree because they were incapacitated, written documentation from the government authority that the information will not be used against the patient, and that a law enforcement activity dependent on the patient health information would be materially and adversely affected by waiting until the patient is able to agree to the disclosure.

In all other cases, documentation to support legal counsel opinion that the disclosure is required to be reported by law or is expressly authorized by statute or regulation before disclosing patient health information for these purposes; and documentation to either support that the patient or personal representative was promptly informed that such action has been or will be taken or documentation to support the physician's decision not to provide notification because such knowledge would put the patient at risk of serious harm.

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

- **Judicial and administrative proceedings.** A copy of patient health information disclosed by a physician in the course of any judicial or administrative proceeding, as well as the following support documentation:

The order received by the physician from the court or administrative tribunal.
Without an order of the court, written documentation from the requesting party providing the following assurances:

- A good faith attempt has been to provide notice to the patient or personal representative,
- The notice provided sufficient information about the litigation or proceeding to permit the patient or personal representative to raise an objection, and
- The time to raise an objection has elapsed, and
- No objection has been filed or the court or administrative tribunal has resolved filed objections and the requested disclosure is consistent with the resolution.
- A qualified order has been provided to the physician that documents that the protected information shall only be disclosed for the purposes of the litigation or proceeding for which it has been requested, and the protected information (including all copies) shall be returned or destroyed at the end of the litigation or proceeding.

- **Law enforcement activities.**

Wounds and injuries: A copy of patient health information disclosed by a physician in the course of meeting legal reporting requirements of certain types of wounds or injuries.

Legitimate law enforcement inquiry: A copy of the patient health information disclosed by the physician when responding to a legitimate law enforcement inquiry, as well as the written documentation obtained from the law enforcement official defining the legal authority to access such information, the scope of the request, and a statement that de-identified information could not reasonably be used.

Identifying and locating individuals: A copy of the patient health information disclosed by the physician when responding to a legitimate law enforcement inquiry to identify or locate an individual, as well as the written documentation obtained from the law enforcement official defining the legal authority to access such information, and a statement requesting information to be used to identify or locate an individual.

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

Victim of crime: A copy of the patient health information disclosed by the physician in response to a law enforcement request when the patient is a suspected victim of a crime, as well as the following support documents:

Written authorization obtained from the victim or patient representative to release information, or if the patient is unable to agree because of incapacity or other emergency circumstance, written documentation obtained from the law enforcement official that the information is needed to determine whether a crime has been committed against the victim and the information will not be used against the victim; that a law enforcement activity dependent on the patient health information would be materially and adversely affected by waiting until the patient is able to agree to the disclosure; and the physician believes that the disclosure is in the patient's best interest.

Decedents: A copy of the patient health information disclosed by the physician to alert law enforcement officials when the physician suspects that the patient's cause of death was the result of criminal conduct.

Crime on premises: A copy of the patient health information disclosed by the physician to law enforcement officials that is believed to constitute physical evidence of criminal conduct that occurred at the Austin Surgical Clinic location, as well as a statement documenting why the physician believes the protected health information constitutes physical evidence.

Reporting crime in emergencies (This section does not apply to suspected victims of abuse, neglect or domestic violence.) A copy of the statement provided by the physician to law enforcement to alert law enforcement to the commission and nature of the crime; the location of the crime and the victim of the crime, and the identity, description, and location of the perpetrator of the crime.

- **Public health activities.** A copy of the patient health information provided by the physician to a public health authority that is authorized to collect or receive information for the purpose of preventing or controlling disease, injury, or disability; or to a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect.
- **Health oversight activities.** A copy of any correspondence from a health oversight agency requesting access to specified information, as well as a copy of patient health information that is disclosed to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, criminal proceedings or actions; or other activities necessary for appropriate oversight of:

Physician Practice Standards for Privacy of Individually Identifiable Health Information Policies and Procedures

- Government benefit programs to determine beneficiary eligibility.
- Government regulatory programs to determine compliance with program standards or civil rights laws.

- **Specialized government functions.** A copy of any correspondence received from a specialized government function requesting access to specified information, as well as a copy of the patient health information disclosed by the physician to facilitate the following government functions: military and veterans activities; protective services for the president and others; and medical suitability determinations for security clearance purposes.
- **Coroners and medical examiners.** A copy of any correspondence received from a coroner or medical examiner requesting access to specified information, as well as a copy of the patient health information disclosed by the physician to the coroner or medical examiner for the purposes of identifying a deceased person, determining a cause of death, or other duties as authorized by law.
- **Funeral directors.** A copy of any correspondence received from a funeral director requesting access to specified information to carry out their duties, as well as a copy of the patient health information disclosed to the funeral director to carry out their duties.
- **Workers compensation insurance.** A copy of patient health information disclosed by Physician Practice to comply with laws relating to workers' compensation or other such programs established by law that provide benefits for work-related injuries or illness without regard to fault.

PROCEDURES:

1. The Privacy Officer shall establish a Notice of Privacy Practices for protected health information that includes information of an individual's right to an accounting of disclosures of their protected health information (see HIPAA Policy 3000).
2. Requests for an accounting of disclosed health information must be submitted in writing by the individual.
3. The patient registration staff shall serve as the contact person for handling these requests. The first accounting in any 12 month period will be provide free of charge. Other accountings will be charged a \$50 fee that must be collected before initiating the accounting process.
4. The Privacy Officer must act upon the request within 60 days of the receipt of the request. A one-time 30-day extension is available if the physician provides written notice of the cause of the delay and the date that the action will be completed.

**Physician Practice
Standards for Privacy of Individually Identifiable Health Information
Policies and Procedures**

5. The accounting of disclosed information must include the following information:
- The date of the disclosure.
 - The name of the person or entity who received the information, and the address of the person or entity, if known.
 - A brief description of the disclosed information.
 - Either provide a brief statement of the purpose for the disclosure that reasonably explains the basis for the disclosure, or provide a copy of the written request to obtain the protected health information.
6. The Privacy Officer or his assignee shall be responsible for completing the accounting, and the Privacy Officer shall be responsible for reviewing and communicating the results of the accounting to the individual.

Effective Date: _____

Physician Practice, Privacy Officer