Summit Physician Specialists, PC

HIPAA
Privacy Manual

Authored by J. Kevin West

TABLE OF CONTENTS

INTRODUCTION

Applicability of this Manual

Summit Physician Specialists, PC, provides many or most of its services in a hospital setting under the control and policies of the hospital. In such situations, Practice personnel will follow hospital policies and this Manual will not apply unless otherwise stated herein. In the non-hospital setting, the policies in this Manual will apply.

Commonly Used Terms

The following abbreviations and shorthand expressions will be used for ease of reference in this Manual:

HHS	Health and Human Services
Practice	The practice or office which implements or uses this Manual.
Practice personnel	All personnel, including physicians, whether owners or otherwise, and their staff, in the practice.
Patient health information	"Protected Health Information," as defined by HIPAA (see Glossary of Terms)
Manual	This HIPAA Privacy Manual
HIPAA	Health Insurance Portability and Accountability Act of 1996

POLICIES AND PROCEDURES

Section A: Workforce Policies

Section B: General Policies Regarding Disclosure of Patient Health Information

Section C: Disclosures Without Patient Authorization

Section D: Patient Rights

Section E: Organizational Matters

Section A:
Workforce Policies

1. Personnel Designations

1.1 **Privacy Officer.** The Practice will designate a person to act as its privacy officer. The privacy officer will have responsibility for the overall implementation and oversight of the Practice's compliance with the HIPAA Privacy Rules. Specifically, the privacy officer will:

- Oversee the implementation of the policies and procedures contained in this Manual.
- Ensure that all Practice personnel are trained regarding the policies and procedures in this Manual as appropriate for their positions and job functions.
- Provide a copy of this Manual to all Practice personnel and ensure that such personnel follow the policies and procedures contained herein.
- Investigate and respond to patient complaints pursuant to Section E.2, and take appropriate action in response.
- Receive and respond to patient requests under the Patient Rights provisions in Section D.
- Maintain all documentation required by this Manual and the HIPAA Privacy Rules.

1.2 **Contact Person.** The Practice will designate a "contact person," to whom patients may make inquiries or submit complaints regarding the Practice's privacy policies, procedures or conduct. The Practice may choose to have its privacy officer and contact person be the same person. The Practice's Notice of Privacy Practices will state the name of its privacy officer and contact person.

2. Training of Practice Personnel

2.1 **Training – Generally.** The Practice will train all Practice personnel regarding the HIPAA Privacy Rules, as well as this Manual, as necessary and appropriate for personnel to carry out their respective job duties.

2.2 **Time for Completion of Training.** Initial training of existing Practice personnel will be completed prior to April 1, 2020. Training of employees hired after April 1, 2020, will be completed within thirty (30) days of hiring. Ongoing training will be provided to Practice personnel as necessary to maintain competency regarding HIPAA policies and procedures, or as needed for changes in the HIPAA Privacy Rules or this Manual.

2.3 **Documentation of Training.** Training of Practice personnel will be recorded in the Privacy Training and Education Log (Appendix E), and this log will be maintained by the Practice for a minimum of six (6) years.

2.4 **Methods of Training.** The Practice owners and privacy officer will use their discretion as to the method, location and frequency of training. Such training may, however, include some or all of the following:

- In-service meetings among Practice personnel.
- Review of this Manual.
- Attendance at programs and seminars.
- Review of professional literature and publications.
- Use of Internet resources (Appendix I).
- Retained consultants and professional advisers.

3. Workforce Discipline

3.1 **Enforcement of Privacy Policies.** All Practice personnel are expected to adhere to the policies and procedures set forth in this Manual. Employees who violate the provisions of this Manual will be subject to discipline, which may include:

- A written warning in the employee's personnel file.
- Placement on probation.
- Mandatory additional training regarding the HIPAA Privacy Rules.
- Demotion or reassignment of job duties.
- Termination.

The privacy officer will maintain a record of all disciplinary action for a minimum of six (6) years.

3.2 **Reporting of Privacy Violations.** Practice personnel are encouraged to report any violation of the provisions of this Manual to the privacy officer. The Practice will not retaliate against any employee for reporting a privacy violation or for supporting a patient's privacy rights.

3.3 **Prevention of Further Violations.** To the extent that privacy violations or deficiencies are reported or discovered, the Practice will take reasonable steps to ensure that similar violations do not occur in the future.

Section B:
General Policies Regarding Disclosure of Patient Health Information

1. General Statement

The Practice will not use or disclose patient health information except as allowed by the HIPAA Privacy Rules, other federal and state laws, and the provisions of this Manual.

2. Patient Authorization

2.1 **General Statement.** Except in those situations described in Section C of this Manual, patient health information may not be disclosed unless a written authorization has been signed by the patient.

2.2 **Valid Authorizations.** To be a valid authorization, the authorization must:

- Be in writing;
- Be signed and dated by the patient or his/her authorized representative;
- Not have expired or been revoked;
- Be filled out completely;
- Contain language required by HIPAA; and
- Not be combined with, or a part of, any other document.

2.3 **Form of Authorization.** Practice personnel shall ensure that patient authorizations are in a form the same as or similar to that found in Appendix C, or that the authorization have the same or similar content as Appendix C.

2.4 **Revocation of Authorization.** A patient may revoke his/her authorization at any time, so long as the revocation is in writing and signed by the patient.

2.5 **Copy to the Patient.** The patient must be given a copy of all authorizations he/she signs.

3. Verification

3.1 **General Statement.** Prior to disclosing patient health information, Practice personnel should verify the identity and authority (where applicable) of the person or entity requesting the information.

3.2 **Verification Protocols.** The following verification protocols will be followed by Practice personnel prior to making disclosures of patient health information:

3.2.1 As to patients:

3.2.1.1 If the patient appears in person and is known to Practice personnel, no verification is necessary; or

3.2.1.2 If the patient appears in person and is not known to Practice personnel, verification should be obtained by requesting photo identification, such as a driver's license; or

3.2.1.3 If a person purporting to be a patient calls the Practice, the identity of the person should be accomplished by asking simple identifying questions such as date of birth, Social Security number or mother's maiden name.

3.2.2 As to law enforcement or other public officials:

3.2.2.1 If the request is made in person, Practice personnel should request to see the officer's or official's identification badge or official credentials; or

3.2.2.2 If the request is made in writing, it is sufficient if it is on appropriate government letterhead; or

3.2.2.3 If the request is made by a person acting on behalf of a public official, Practice personnel should obtain a written statement on appropriate government letterhead showing the authority of the person making the request.

Patient health information will not be given by telephone to law enforcement or public officials except as provided in Section C.5.

3.2.3 As to health care providers who are treating the patient or insurance companies paying for treatment:

3.2.3.1 If the health care provider or insurance company is known to the Practice, no further verification is necessary; or

3.2.3.2 If the health care provider or insurance company is not known to the Practice, a written request (by fax or mail) on their letterhead shall be requested for verification.

3.3 **Documentation.** To the extent that verification is required by subsection 3.2, such will be documented or noted in the patient's chart.

4. Limiting Disclosures and Requests to the Minimum Necessary Information

4.1 **General Rule.** The Practice will make reasonable efforts to limit its disclosures of, and requests for, patient health information to the minimum necessary information needed to accomplish the purpose of the disclosure or request. Except as allowed below, the Practice will not request or disclose the patient's entire medical record unless such is justified to accomplish the purpose of the request.

4.2 **Information Requests Received By the Practice.**

4.2.1 Whenever possible, the Practice will redact or delete the following items from the information disclosed to others:

- Names;
- Postal address information, other than town or city, state, and zip code;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social Security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints; and
- Full face photographic images and any comparable images;

If the above items are not deleted, the Practice should document the reason for such.

4.2.2 For health information requests received by the Practice on a routine and reoccurring basis, the Practice will develop and follow protocols that limit the information disclosed to that which is reasonably necessary to achieve the purpose for the request;

4.2.3 For all other requests, the Practice will develop and follow criteria designed to limit the information disclosed to that which is reasonably necessary to achieve the purpose of the request, and will review the request on an individual basis in accordance with that criteria.

4.3 **Requests Made By the Practice to Others for Information.**

4.3.1 For health information requests made by the Practice to others on a routine and reoccurring basis, the Practice will develop and follow standard protocols that limit the information requested to that which is reasonably necessary to achieve the purpose for the request;

4.3.2 For all other requests, the Practice will develop and follow criteria designed to limit the information requested to that which is reasonably necessary to achieve the purpose of the request, and will review the request on an individual basis in accordance with that criteria.

4.4 **Exceptions.** Practice personnel will not be required to follow the rules stated above in the following situations:

- Disclosures or requests to a health care provider for purposes of treatment.
- Disclosures to the patient.
- Disclosures or requests made pursuant to the patient's written authorization.
- Disclosures to Health and Human Services (HHS).
- Disclosures required by the HIPAA Privacy Rules.
- Disclosures required by law (see Section C.4).

4.5 **Minimum Necessary Workforce Access to Patient Health Information.** Practice personnel who do not have a legitimate need to have access to patient health information to carry out their duties shall be restricted from having such access. The privacy officer will determine, in his/her discretion, whether access should be denied to any Practice personnel.

5. Health Information of Deceased Patients

5.1 **General Statement.** Health information of deceased patients will be given the same protections as health information of living patients. However, health information of deceased patients who have been dead for more than 50 years is no longer protected by HIPAA.

5.2 **Executors and Personal Representatives.** Legally authorized executors or personal representatives of deceased patients are entitled to act on behalf of the deceased patient with respect to the patient's health information. All patient rights and protections set forth in this Manual must be afforded to such executors or personal representatives.

5.3 **Family Members and Close Personal Friends.** The Practice may disclose patient health information to a deceased patient's family members or close personal friends, but only to the extent that the information is related to that person's involvement in the deceased patient's care, and sharing the information would not be inconsistent with the deceased patient's expressed wishes. For purposes of this section, "family member" includes spouses, children, parents, siblings, grandparents, grandchildren, aunts, uncles, nephews, nieces and cousins.

6. Disclosures for Workers' Compensation Purposes

Disclosures of patient health information for purposes of workers' compensation benefits may be made pursuant to state workers' compensation laws and regulations.

7. Sale of Patient Records

The Practice will not sell patient records to a third party unless –

- The patient has consented in writing; or
- The Practice is being sold to another health care provider who is a covered entity under HIPAA regulations.

Section C:
Disclosures Without Patient Authorization

1. General Statement

1.1 **Disclosures Allowed Without Patient Written Authorization.** In the following circumstances, the Practice may disclose patient health information without the patient's written authorization:

1.1.1 To the patient himself/herself, upon request.

1.1.2 To other persons or entities for purposes of:

- The Practice's treatment (as defined in Appendix H) of the patient.
- Obtaining payment (as defined in Appendix H) for the Practice's services.
- The Practice's "health care operations" (as defined in Appendix H).

1.1.3 To another health care provider for the purpose of that provider's treatment of the patient.

1.1.4 To other health care providers or HIPAA covered entities (as defined in Appendix H) for the purpose of their making or obtaining payment for health care services provided to the patient.

1.1.5 To another HIPAA covered entity (as defined in Appendix H), but only if that entity either has or had a relationship with the patient whose health information is being requested, the information requested pertains to that relationship, and the information is for the purpose of the following "health care operations":

1.1.5.1 Conducting quality assessment and improvement activities, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination; contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment; or

1.1.5.2 Reviewing the competence or qualifications of health care professionals; evaluating practitioner and provider performance, or health plan performance; conducting training programs in which students, trainees or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers; training of non-health care professionals; accreditation, certification, licensing or credentialing activities.

2. Disclosures to Parents and Other Authorized Representatives

2.1 **Guardians and Conservators.** If, under Utah law, a person has legal authority to act for the patient as a guardian, conservator or holder of a power of attorney, the Practice may treat that person as if he/she is the patient as to all matters within the scope of that representative's authority. Practice personnel will request documentation (and keep a copy in the patient's file) from the representative to verify their authority to act on behalf of the patient.

2.2 **Parents of Unemancipated Minors.** If, under Utah law, a parent or other person acting *in loco parentis* (a guardian or temporary custodian, foster parent, etc.) of an unemancipated minor has authority to act for the minor in making decisions related to health care, the Practice may treat that person as if he/she is the patient and will grant him/her the same rights and protections set forth in this Manual. As to guardians, foster parents or temporary custodians, Practice personnel will request documentation (and keep a copy in the patient's file) to verify their authority to act on behalf of the patient.

2.3 **Domestic Violence, Abuse or Neglect.** The Practice may decline to recognize a guardian, conservator, parent or other personal representative if, under Utah law, the Practice has reason to believe that the patient has been or may be subjected to domestic violence, abuse or neglect by that person, or that recognizing such a person as the patient's representative could endanger the patient.

2.4 **Rights of Minors Under State Law.** If Utah law allows an unemancipated minor to consent to obtain health care without parental consent, the Practice will not treat the parent as the minor's representative.

3. Disclosures to Close Friends and Family Members

3.1 **General Statement.** In the situations described below, Practice personnel may disclose patient health information to family members, relatives or close personal friends of the patient.

3.2 **Disclosures to Family Members or Closer Personal Friends.** Practice personnel may disclose to family members, relatives or close personal friends of the patient that health information directly relevant to such person's involvement in caring for the patient or paying for the patient's care if:

- The patient is physically present at the time of the disclosure and either agrees verbally or does not object to the disclosure, or Practice personnel reasonably infer from the circumstances that the patient does not object; or
- The patient is not physically present or is incapacitated (unconscious, sedated, etc.) and Practice personnel determine that a disclosure of limited information would be in the patient's best interests. For example, Practice personnel may make limited disclosures to allow family, friends or relatives to pick up filled prescriptions, medical supplies, X-rays or similar items for the patient if Practice personnel determine that such would be in the patient's best interests.

3.3 **Other Disclosures to Caregivers.** Practice personnel may disclose patient health information to locate and notify a family member, personal representative or other person responsible for the patient's care of the patient's location, general condition or death if:

- The patient is physically present at the time of the disclosure and either agrees verbally or does not object to the disclosure, or Practice personnel reasonably infer from the circumstances that the patient does not object; or
- The patient is not physically present, is incapacitated (unconscious, sedated, etc.) or deceased, and Practice personnel determine that a disclosure of limited information would be in the patient's best interests.

4. Disclosures Required by Law

4.1 **General Statement.** In certain circumstances, as described below, Practice personnel may disclose patient health information when required by law to do so. In such situations, the disclosure of patient health information should always be limited to only that which is required by law.

4.2 **Public Health Reporting.** Patient health information may be disclosed to:

- A public health authority that is authorized to receive information for the purpose of preventing or controlling disease, injury or disability (e.g., reporting of communicable diseases, births, deaths, etc.).
- A public health authority or other appropriate government authority authorized to receive reports regarding suspected child abuse or neglect (as defined by state law).
- Drug company representatives or medical device company representatives regulated by the FDA, for purposes of (1) reporting adverse events involving the drug or device; (2) tracking FDA related products; (3) enabling product recalls, repairs or replacements; or (4) conducting post marketing surveillance.
- A person who may have been exposed to a communicable disease or who may be at risk of contracting a disease or condition, if state law authorizes the Practice to notify the person as part of a public health investigation or intervention.

4.3 **Victims of Abuse, Neglect or Domestic Violence.** Practice personnel may disclose patient health information regarding a patient believed to be the victim of abuse (other than child abuse), neglect or domestic violence to a government authority authorized by law to receive reports of such abuse, neglect or domestic violence where:

- The disclosure is required by state law;
- The patient agrees to the disclosure; or
- The disclosure is allowed by state law and Practice personnel believe the disclosure is necessary to prevent serious harm to the patient or other potential victims, or the patient is incapacitated and a law enforcement officer or authorized public official states that the information will not be used against the patient and that waiting for the information would adversely impact immediate enforcement activity.

If a disclosure of patient health information is made for the reasons described in this subsection 4.3, the patient must be informed that the disclosure has been or will be made unless informing the patient would put him/her at risk of serious harm. Practice personnel need not inform a parent, guardian, conservator or other personal representative of the disclosure if it is reasonably believed that such a person is responsible for the abuse, neglect and domestic violence, and that informing them would not be in the patient's best interests.

4.4 **Health Oversight Activities.** Practice personnel may disclose patient health information to federal or state agencies for purposes of :

- audits;
- civil, administrative or criminal investigations or proceedings;
- inspections; or
- licensure or disciplinary actions;

relating to oversight of the health care system, government benefit programs and regulation of government programs for which health information is necessary.

4.5 **Judicial and Administrative Proceedings.** Practice personnel may disclose patient health information in relation to a judicial or administrative proceeding —

4.5.1 When ordered to do so by a court or administrative tribunal; or

4.5.2 Upon receipt of a subpoena or discovery request if –

4.5.2.1 The Practice receives an appropriate protective order from the court or tribunal that prohibits the parties to the case from using or disclosing the information for any purpose other than the proceeding, and requires the return to the Practice or destruction of the health information at the end of the proceeding; or

4.5.2.2 The patient has been notified in writing of the request for his/her health information, and the notice gave the patient sufficient information about the proceeding in order to allow the patient to raise an objection to the court or tribunal by a certain date, and the patient has not objected to the disclosure within the specified time period, or the court/tribunal has resolved the patient's objections.

4.6 **Law Enforcement.**

4.6.1 **Disclosures required by orders, warrants or subpoenas.** Practice personnel may disclose patient health information to a law enforcement official for law enforcement purposes in the following situations:

- Where state law requires the reporting of certain types of wounds or injuries (e.g., gunshot wounds);
- Upon receipt of a court order or court-ordered warrant;
- Upon receipt of a subpoena or summons issued by a judicial officer;
- Upon receipt of a grand jury subpoena; or
- Upon receipt of an administrative subpoena, summons or investigative demand.

4.6.2 **Identification of suspects, fugitives or witnesses.** Other than in those situations described in subsection 4.6.1, above, Practice personnel may disclose only the following limited patient health information to law enforcement officials in

response to their request made for purposes of identifying or locating a suspect, fugitive, material witness or missing person:

- 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
- A description of distinguishing physical characteristics

4.6.3 **Patients who are crime victims.** Practice personnel may disclose patient health information to a law enforcement official about a patient who is the victim of a crime if:

- The patient agrees to the disclosure; or
- The Practice is unable to obtain the patient's agreement due to his/her incapacity and the law enforcement official states that the information is needed to determine whether a crime was committed by someone other than the patient, immediate action depends upon the disclosure, and disclosure would be in the patient's best interests.

4.7 **Coroners and Funeral Directors.**

4.7.1 Practice personnel may disclose health information of a deceased patient to a coroner for the purpose of identifying a deceased person, determining the cause of death or other duties authorized by law.

4.7.2 Practice personnel may disclose health information of a deceased patient to a funeral director pursuant to applicable state law.

5. Disclosures to Prevent Serious Threats to Health or Safety

5.1 Unless otherwise prohibited by state law or professional ethical standards, Practice personnel may disclose patient health information if such disclosure —

5.1.1 Is necessary to prevent a serious and imminent threat to the health or safety of a person or the public, and is made to someone reasonably able to prevent the threat, including the target of the threat; or

5.1.2 Is necessary for law enforcement authorities to identify or apprehend the patient —

5.1.2.1 because of a statement by the patient admitting participation in a violent crime that caused serious physical harm to the victim; or

5.1.2.2 where it appears that the patient has escaped from a correctional institution or from law custody.

5.2 A disclosure made pursuant to subsection 5.1.2.1, above, must be limited to only the patient's statement and the following 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
- A description of distinguishing physical characteristics

6. Disclosures to Business Associates

6.1 **Definition of Business Associates.** "Business associates" are third parties who create, receive, transmit or maintain patient health information on behalf of the Practice. (Examples include: data storage companies, IT vendors and service providers, transcriptionists, billing services, clearinghouses, attorneys, accountants, collection agencies, etc.) Other treating health care providers are not business associates. (A more extensive definition may be found in Appendix H.)

6.2 **Requirement for Business Associate Agreements.** The Practice may disclose patient health information to its business associates if and only if the business associate has signed an agreement to protect patient privacy by following HIPAA Privacy Rules.

6.3 **Time for Obtaining Business Associate Agreements.**

6.3.1 If possible, the Practice shall have all of its current business associates sign an agreement the same as or similar to that found in Appendix B to this Manual prior to March 1, 2020.

6.3.2 Those business associates with whom the Practice forms a relationship after March 1, 2020, must sign an agreement the same or similar to that found in Appendix B. Patient health information may not be disclosed to business associates who fail or refuse to sign agreements by these dates.

6.4 **Privacy Violations by Business Associates.** If the Practice or any of its personnel become aware that a business associate has violated or is violating its obligations under the business associate agreement, the Practice shall:

- Contact the business associate and request that such violations cease immediately; or
- If the request to cease violations is not followed, terminate its relationship with the business associate.

7. Other Disclosures Which May Not Require Patient Authorization

7.1 **Research**. The practice may use or disclose patient health information for purposes of research projects provided that —

- The Practice obtains documentation that a waiver of patient authorization has been approved by either (1) an institution of review board (IRB) established pursuant to federal law, or (2) a privacy board composed of members with varying backgrounds and appropriate professional competency as necessary to review research protocols, and the board has at least one member who is not affiliated with the Practice or any entity conducting the research;
- The Practice obtains from the researcher a signed statement that patient health information is sought solely to prepare a research protocol or for similar purposes preparatory to research and that no health information will be removed from the Practice by the researcher in the course of his/her review; and
- The IRB or privacy board has determined that there is a minimal privacy risk to patients, there is an adequate plan to protect patient identifying information, and there is an adequate plan to destroy patient identifiers at the appropriate time consistent with the research.

7.2 **Marketing.**

7.2.1 **General statement.** "Marketing" means communications about a product or service that encourages someone to buy or use the product or service.

7.2.2 **Face to Face Communications with Patients.** Practice may have face-to-face communications with patients regarding its own services as well as the products and services of third parties.

7.2.3 **Marketing activities that do not require authorization.** The Practice may engage in the following marketing activities (as defined in 7.2.1) without obtaining patient authorization, so long as the Practice is not paid by a third party to make such communications:

- Communications to patients regarding their treatment;
- Communications regarding the case management or coordination of care of the patient; or
- Recommendations to the patient regarding alternative treatments, therapies or health care providers.

7.2.3 Other than those activities described in subsection 7.2.2 and 7.2.3, marketing activities require written patient authorization.

7.3 **Fundraising Activities.**

7.3.1 The Practice will not send fundraising communications to patients unless –

- Such communications include a clear and conspicuous statement of how the patient may opt-out of receiving further communications, and
- Such communications state that treatment of the patient will not be contingent upon the patient agreeing to receive fundraising communications.

7.3.2 The Practice will not send out fundraising communications to any patient who opts out from receiving such.

Section D:
Patient Rights

1. General Statement

Practice personnel will recognize, uphold and enforce all patient rights established by the HIPAA Privacy Rules, and as set forth in this Section D of the Manual.

2. Right to Notice

Patients of the Practice have a right to receive a notice of the Practice's privacy policies and procedures. The Practice will prepare and post a notice of privacy practices. This notice will be provided to patients whose first encounter with the Practice is in a non-hospital setting. The notice will be posted in the Practice's lobby or reception area (in non-hospital settings) in a location accessible to all patients. If the Practice maintains a website, the notice of privacy practices will be posted on the website.

3. Right to Request Restrictions

3.1 **General Statement.** Subject to the statement of applicability on page 1 of this Manual, patients have a right to request that the Practice restrict the uses or disclosures of patient health information to carry out treatment, payment or health care operations, and have a right to request that the Practice restrict disclosures made to family, relatives and close personal friends.

3.2 **Written Request.** Patients who request restrictions on the use or disclosure of their health information will be asked to fill out the Restriction Request Form as found in Appendix K.

3.3 **Procedure.** If the Practice receives a written request to restrict the uses and disclosures of patient health information, the request will be referred to the privacy officer for handling. The privacy officer will notify the patient in writing within a reasonable time as to whether the Practice will agree to the restriction. If the privacy officer advises the patient that it will not agree to the restriction, no further action is necessary. If the Practice advises the patient that it will abide by the restriction, a notation will be made prominently in the patient's chart, and the Practice will abide by that restriction from that date forward.

3.4 **Disclosures Required by Law.** The Practice will not agree to restrict disclosures of health information that are required by law.

3.5 **Termination of Restrictions.** If the Practice has agreed to a restriction on uses or disclosures of health information, it may terminate that agreement by advising the patient in writing that the termination will only be effective with respect to health information created or received after written notification to the patient. As to health information created or received prior to that date, the restriction must be followed.

3.6 **Documentation.** All patient requests for restrictions, along with the Practice's response thereto, shall be kept for a minimum of six (6) years from the date of the document(s).

4. Right to Confidential Communications

4.1 **General Statement.** Subject to the statement of applicability on page 1 of this Manual, patients have a right to request reasonable accommodations in receiving communications of their health information by alternative means or at alternative locations.

4.2 **Written Request.** Patients who request confidential communications will be asked to fill out the Request for Confidential Communications form, as found in Appendix L.

4.3 **Procedure.** Upon receipt of a request for confidential communications, the privacy officer will evaluate the request. If the request is reasonable, the privacy officer will note the request prominently in the patient's chart and adhere to the request. For example, if the patient requests that all communications be sent to an address different than the patient's home address, the Practice will adhere to that request and note it in the patient's chart. If the request is not reasonable, the privacy officer will notify the patient that the request has been rejected.

4.4 **Conditions to Providing Confidential Communications.** As a condition to providing confidential communications at the patient's request, the Practice may require that the patient provide assurances as to how payment for services will be provided.

4.5 **No Demand for Explanations.** The Practice may not require an explanation from patients as to the reason for requesting confidential communications.

4.6 **Documentation.** All patient requests for confidential communications, along with the Practice's response thereto, shall be kept for a minimum of six (6) years from the date of the document(s).

5. Right to Access

5.1 **General Statement.** Patients have a right to inspect and obtain a copy of their health information in the designated record set (as defined in Section E.6), except as noted herein.

5.2 **Procedure.** The practice may require that the patient request in writing to have access to his/her health information. Upon receipt of such a request, the Practice will provide the patient with an opportunity to inspect his or her health information and obtain a copy (paper or electronic) within the following time frames:

- For records that are maintained on site, the Practice will provide access and copies within 30 days from the receipt of the request from the patient;
- If the Practice is unable, despite good faith efforts, to provide access within 30 days, it may have a one-time extension of an additional 30 days to provide access and copies if the patient is notified in writing of the reasons for the delay and the expected date that access/copies will be provided.

5.2.1 The Practice will provide the patient with the health information in readable hard copy form. If the Practice maintains health information in electronic form, and the patient requests access to the health information in electronic form, the Practice will provide the information in the format requested if possible. If this is not possible, the Practice will provide access in a format (e.g., PDF, Word, Excel) mutually acceptable to the patient and the Practice. If the patient requests that the health information be sent to him/her in an email, the Practice may do so if it first warns the patient that there is some level of risk that the information could be intercepted and read by a third party. If the patient requests that the Practice transmit a copy of the health information directly to a third party, in paper or electronic form, the Practice will comply with this request. The Practice may provide the patient with a summary of the health information in lieu of providing access to the records themselves if and only if the patient agrees to receiving a summary and the patient agrees in advance to paying the fees imposed, if any, for the Practice providing the summary.

5.2.2 The Practice will provide a convenient time and place for the patient to inspect his/her health information or to obtain a copy of the information.

5.2.3 The Practice may charge a reasonable, cost-based fee for copies and preparing, producing and providing the patient with copies of his/her health information. That fee may include copying charges, including the cost of supplies, electronic media, and labor for copying, burning to disk, scanning or transmitting the information. The Practice may also charge postage if the patient has requested that the information be mailed. If the patient has agreed to a summary, the Practice may charge the costs of preparing the summary. The Practice may not charge a retrieval fee to find or obtain the requested health information. If state

law limits the amount that may be charged for copies, the Practice may not charge in excess of that amount.

5.2.4 All requests by patients for access to health information will be referred to the privacy officer. In those circumstances in which access to health information is denied, the privacy officer will determine if some part of the patient's record may be disclosed without objection. If so, that portion of the record may be disclosed. As to all other parts of the record for which access is denied, the privacy officer will provide a timely, written denial to the patient stating the basis for the denial and, if applicable, the patient's right to have the denial reviewed. The written notice must also explain to the patient that they may complain regarding the denial of access either to the Practice or to the Secretary of HHS. This notice will include the name, title and telephone number of the privacy officer.

5.2.5 All documentation regarding patient requests for access and any denials thereof, or any other documentation maintained under this subsection, must be retained by the Practice for a minimum of six (6) years from the date of the document(s).

5.3 **Denial of Access.**

5.3.1 **Unreviewable grounds for denial.** The Practice may deny patients access to health information that is created, maintained or is otherwise subject to the Clinical Laboratory Improvements Amendments of 1988 (CLIA) to the extent that providing access would be prohibited by that law, or where such information is made exempt under the CLIA law. In addition, a patient who is part of a research program may have his/her right of access temporarily suspended for as long as the research is in progress, provided that the patient has agreed to the denial of access at the time that he/she consented to participate in the research.

5.3.2 **Reviewable grounds for denial of access.**

5.3.2.1 The Practice may deny the patient access to his/her health information if the Practice reasonably believes that such access is likely to endanger the life or physical safety of the patient or another person, or that the information makes reference to another person and the Practice believes that allowing access may cause substantial harm to that person.

5.3.2.2 The Practice may deny access to a guardian, conservator or parent where the practice believes that such person is likely to cause substantial harm to the patient or another person by having access to the patient's health information.

5.3.2.3 If access to the patient's health information is denied for the above reasons, the patient has a right to have the denial reviewed by a licensed healthcare professional designated by the Practice as a

reviewing official. This health care professional must be someone who did not participate in the original decision to deny access. The Practice will abide by the decision of that reviewing health care professional, to either grant or deny access to the patient.

6. Right to Amend

6.1 **General Statement.** Subject to the statement of applicability on page 1 of this Manual, patients have a right to request that the Practice amend their health information in the designated record set (as defined in Section E.6).

6.2 **Procedure.** The Practice will follow the following procedures when a request to amend is received from a patient.

6.2.1 **Written request.** Patients who request amendments or corrections to their health information will be asked to fill out the Request for Correction/Amendment of Health Information form, as found in Appendix J. The requests will be referred to the privacy officer.

6.2.2 **Response to the patient's request.** After a reasonable investigation, the privacy officer will determine whether the practice will grant or deny the request to amend. The privacy officer will respond in writing to the patient's request within 60 days from the date of the request by either granting the amendment, or advising the patient of the denial of the request, as described below.

6.2.2.1 **Acceptance of amendment.** If the Practice accepts the patient's request for amendment, it will amend the patient's record and provide an appropriate link or reference to the location of the amendment. The Practice will also make reasonable efforts to provide the amendment within a reasonable time to those persons identified by the patient as having received health information about the patient and who need the amendment, and those persons, including business associates, who the Practice knows may have relied upon the information that is subject to the amendment.

6.2.2.2 **Denial of amendment.** If the Practice determines to deny an amendment, it must provide the patient with a timely, written denial stating the basis for the denial, the patient's right to submit a statement disagreeing with the denial and how the patient may file that statement. In addition, the Practice must inform the patient that he/she may request that the Practice provide a copy of the patient's request for amendment and the denial with any future disclosures of health information regarding the patient. The Practice must advise the patient that he/she is entitled to make a complaint and how such complaints may be submitted to the Practice or Secretary of HHS. This notice must include the name or title and telephone number of the Practice's privacy officer. If the patient, upon denial of the request to amend, submits a written statement disagreeing with the denial, the Practice must include such statement with the patient's records and include that

statement with any subsequent disclosure of the patient's health information to which the disagreement relates.

6.2.3 The Practice may deny a patient's request for amendment if the privacy officer determines that the health information subject to the request —

- was not created by the Practice;
- is not part of the patient's chart;
- would not be available for inspection under the provisions of this Manual; or
- is accurate and complete.

6.3 **Documentation.** All patient requests to amend their health information, along with the Practice's response thereto, shall be kept for a minimum of six (6) years from the date of the document(s).

7. Right to an Accounting

7.1 **General Statement.** Subject to the statement of applicability on page 1 of this Manual, patients have a right to receive an accounting of disclosures of their health information made by the Practice and its business associates as set forth below.

7.2 **Procedure.** Patients requesting an accounting will be asked to make the request in writing. All requests for an accounting will be referred to the privacy officer. In responding to such requests, the privacy officer will follow the following procedures:

7.2.1 The privacy officer will respond to the patient's request no later than 60 days from the receipt of the request by providing the patient with a written accounting using the appropriate form in Appendix G (for electronic and non-electronic health information).

7.2.2 The Practice will retain a copy of all requests for accountings from patients as well as the accounting provided by the Practice to the patient for a minimum of six (6) years from the date of the document(s).

7.3 **Suspension of the Right to an Accounting.** The Practice may temporarily suspend the patient's right to receive an accounting of disclosures made to a health oversight agency or a law enforcement official for the time specified by that agency or official if giving the accounting would impede the agency's activities.

7.4 **Exceptions for Non-Electronic Health Records.** Patients shall have no right to an accounting as to disclosures of non-electronic health information —

- To carry out treatment, payment or health care operations (as defined in Appendix H);
- To the patient;
- Incident to a use or disclosure otherwise permitted by this Manual or the HIPAA Privacy Rules;
- Pursuant to an authorization signed by the patient;
- To correctional institutions or law enforcement officials; or
- That occurred prior to April 14, 2003.

7.5 **Electronic Health Records.** If the Practice maintains health information in electronic form, the exceptions stated in subsection 7.4 do not apply.

7.5.1 The Practice is only required to give an accounting for disclosures of electronic health records which occurred within three (3) years of the patient's request.

7.5.2 The Practice must contact any Business Associates who have the patient's health information in electronic form and request that they provide the Practice with an accounting of all disclosures of the patient's electronic health information.

7.5.3 Alternatively, the Practice can provide an accounting of the disclosures it made and give the patient a list of all Business Associates (including contact information) who may possess the patient's health information in electronic form.

7.5.4 This section 7.5, and all subparts, applies only to disclosures of electronic health information that occur after January 1, 2011 [after January 1, 2014, for practices that had an EHR prior to January 1, 2009].

8. Waivers of Patient Rights and Non-Retaliation

8.1 **No Waivers of Privacy Rights.** No patient or prospective patient will be asked to waive their rights under the HIPAA Privacy Rules as a condition to receiving health care services from the Practice.

8.2 **Non-Retaliation Policy.** Practice personnel will not intimidate or retaliate against patients who seek to inquire about, enforce or complain regarding their rights under the HIPAA Privacy Rules or this Manual.

Section E:
Organizational Matters

1. Notice of Privacy Practices

1.1 **Preparation of the Notice.** The Practice will prepare a Notice of Privacy Practices the same or similar to that found in Appendix A. The Notice will contain those provisions required by the HIPAA Privacy Rules, and will be in two sections: a summary and an attached Notice of Privacy Practices (Notice). The entire Notice will be provided to patients in the non-hospital setting.

1.2 **Providing the Notice to Patients.** The Practice will provide the Notice to each new patient who comes to the Practice in a non-hospital setting after March 1, 2020; for existing patients, the Practice will provide the Notice at the time of the patient's first visit to the Practice after March 1, 2020.

1.3 **Posting the Notice.** The Notice will be posted or located prominently in the Practice's non-hospital lobby or reception areas. If the Practice has multiple offices or other locations where health care is provided, the Notice will be posted in each location. If the Practice has a website, the Notice will be posted on the website.

1.4 **Patient Acknowledgment.** Practice personnel will make a good faith effort to have each patient acknowledge in writing his/her receipt of the Notice at the time the Notice is provided pursuant to subsection 1.2, above. Acknowledgment may be accomplished by:

- The patient signing and dating a separate acknowledgment form;
- The patient checking off a box on an intake form signed and dated by the patient; or
- The patient initialing/signing and dating the Notice itself.

Notation will be made as to patients who refuse to acknowledge receipt of the Notice.

1.5 **Document Retention.** The Practice will retain patient acknowledgments for a minimum of six (6) years from the date they are signed.

2. Patient Complaints

2.1 **Notice to Patients.** The Practice will notify its patients, through the Notice of Privacy Practices, that they may make complaints regarding the Practice's policies, procedures and practices with respect to the HIPAA Privacy Rules. The Notice will also set forth the complaint process described below.

2.2 **Procedure for Patient Complaints.**

2.2.1 Patient complaints must be submitted in writing to the contact person designated by the Practice using the form in Appendix F.

2.2.2 Patient complaints will be reviewed by the privacy officer, and appropriate investigation, if any, will be conducted to develop the necessary information regarding the complaint.

2.2.3 Within fifteen (15) days of receiving the written complaint, the privacy officer will advise the patient, in writing, of the privacy officer's determination regarding the complaint, and the measures, if any, which will be taken by the Practice to mitigate any improper uses or disclosures of protected health information.

2.2.4 If the patient requests information to make a complaint to HHS, the privacy officer will provide the patient with HHS's address, as follows:

Office of Civil Rights
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Room 509F, HHH Building
Washington, D.C. 20201
(202) 619-0257
Email: ocrmail@hhs.gov

2.3 **Document Retention.** All documentation received or prepared in relation to a patient complaint will be kept a minimum of six (6) years.

2.4 **Non-Retaliation Policy.** Practice personnel will not retaliate against any patient who submits a complaint.

3. Mitigation of Improper Disclosures

If the Practice learns of an improper disclosure of patient health information, either through patient complaint or otherwise, the Practice will take immediate action to mitigate the impact of the disclosure to the extent possible. The Practice will also seek to mitigate, to the extent practicable, any improper disclosures of its business associates. For improper disclosures of patient health information, the Practice will follow the patient notification procedures set forth in Section B of the HIPAA Security Manual.

4. Privacy and Security Safeguards

The Practice will implement administrative, technical and physical safeguards to protect the privacy of patient health information as appropriate to the size, resources and circumstances of the Practice. These safeguards will be implemented as set forth in the Practice's HIPAA Security Manual. In particular, the Practice will take reasonable steps to prevent disclosures of patient health information in the following areas:

- reception and waiting room areas;
- hallways and treatment rooms;
- Patient record storage areas;
- fax machines and photocopiers;
- computer terminals and computer systems;
- portable electronic devices (laptops, PDA's, cell phones); and
- e-mail and other Internet communication.

5. Record Retention and Disposal

5.1 **Policies and Procedures Maintained.** The Practice will keep and maintain policies and procedures designed to ensure compliance with the HIPAA Privacy Rules.

5.2 **Document Retention Period.** The Practice will retain, for a minimum of six (6) years, all records, documents or information generated, created or required to be kept under the policies and procedures in this Manual, or as otherwise required by the HIPAA Privacy Rules.

5.3 **Storage in Secure Locations.** Records and information of the Practice will be kept or stored in safe, secure locations. Practice records stored offsite will be placed only in secure facilities.

5.4 **Disposal of Patient Health Information.** Patient health information (in whatever format or medium) will be disposed of using appropriate methods. Hard copy (paper) records will be disposed of by means of shredding, incineration or other methods that obliterate any identifying information in such records. Hard copy records or other health information will never be disposed of by placing such in a trash receptacle or dumpster.

6. Designated Record Set

6.1 **Matters Included in Designated Record Set.** The designated record set for patient health information shall include the following types of records or information:

- Patient medical files (whether in paper or electronic form);
- Patient financial, billing and collection information (whether in paper or electronic form); and
- Patient health information created or maintained by Business Associates;

to the extent that such is created or maintained for the purpose of making decisions about patients.

6.2 **Matters Not Included in Designated Record Set.** The following records, documents or information (whether in paper or electronic format) shall not be considered part of the designated record set:

- Quality improvement records;
- Risk management records;
- Psychotherapy notes;
- Cancer Registry information;
- Appointment or surgical schedules;
- Information compiled in anticipation of, or preparation for, civil, criminal or administrative proceedings;
- Patient health information exempt under the Clinical Laboratory Improvements Act (CLIA); or
- Other information exempt from disclosure under state or federal law.

APPENDICES

A. Notice of Privacy Practices

B. Sample Business Associate Agreement

C. Patient Authorization to Release Health Information

D. Practice Resolutions

E. Privacy Training and Education Log

F. Patient Complaint Form

G. Accounting of Disclosures Forms

H. Glossary of Terms

I. HIPAA Resources

J. Request for Correction/Amendment of Health Information

K. Restriction Request Form

L. Request for Confidential Communications

M. Quick Reference Regarding Disclosures Requiring/Not Requiring Written Patient Authorization

N. Acknowledgment of Receipt/Review of HIPAA Privacy Manual

APPENDIX A

Notice of Privacy Practices[1]*

[1]* Appendix A includes both a summary notice (one page) as well as a complete Notice of Privacy Practices (four pages). The Practice may use the summary notice together with the complete notice, or may simply use the complete notice alone. It is not sufficient, however, to use only the summary notice alone.

SUMMARY OF NOTICE OF PRIVACY PRACTICES

This summary is provided to assist you in understanding
the attached Notice of Privacy Practices

The attached Notice of Privacy Practices contains a detailed description of how our office will protect your health information, your rights as a patient and our common practices in dealing with patient health information. Please refer to that Notice for further information.

Uses and Disclosures of Health Information. We will use and disclose your health information in order to treat you or to assist other health care providers in treating you. We will also use and disclose your health information in order to obtain payment for our services or to allow insurance companies to process insurance claims for services rendered to you by us or other health care providers. Finally, we may disclose your health information for certain limited operational activities such as quality assessment, licensing, accreditation and training of students.

Uses and Disclosures Based on Your Authorization. Except as stated in more detail in the Notice of Privacy Practices, we will not use or disclose your health information without your written authorization.

Uses and Disclosures Not Requiring Your Authorization. In the following circumstances, we may disclose your health information without your written authorization:

- To family members or close friends who are involved in your health care;
- For certain limited research purposes;
- For purposes of public health and safety;
- To Government agencies for purposes of their audits, investigations and other oversight activities;
- To government authorities to prevent child abuse or domestic violence;
- To the FDA to report product defects or incidents;
- To law enforcement authorities to protect public safety or to assist in apprehending criminal offenders;
- When required by court orders, search warrants, subpoenas and as otherwise required by the law.

Patient Rights. As our patient, you have the following rights:

- To have access to and/or a copy of your health information;
- To receive an accounting of certain disclosures we have made of your health information;
- To request restrictions as to how your health information is used or disclosed;
- To request that we communicate with you in confidence;
- To request that we amend your health information;
- To receive notice of our privacy practices.

If you have a question, concern or complaint regarding our privacy practices, please refer to the attached Notice of Privacy Practices for the person or persons whom you may contact.

Summit Physician Specialists, PC

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 IT CAREFULLY. THE PRIVACY OF YOUR MEDICAL INFORMATION IS IMPORTANT TO US.

Our Legal Duty

We are required by applicable federal and state laws to maintain the privacy of your protected health information. We are also required to give you this notice about our privacy practices, our legal duties, and your rights concerning your protected health information. We must follow the privacy practices that are described in this notice while it is in effect. This notice takes effect March 1, 2020, and will remain in effect until we replace it.

We reserve the right to change our privacy practices and the terms of this notice at any time, provided that such changes are permitted by applicable law. We reserve the right to make the changes in our privacy practices and the new terms of our notice effective for all protected health information that we maintain, including medical information we created or received before we made the changes.

You may request a copy of our notice (or any subsequent revised notice) at any time. For more information about our privacy practices, or for additional copies of this notice, please contact us using the information listed at the end of this notice.

Uses and Disclosures of Protected Health Information

We will use and disclose your protected health information about you for treatment, payment, and health care operations.

Following are examples of the types of uses and disclosures of your protected health care information that may occur. These examples are not meant to be exhaustive, but to describe the types of uses and disclosures that may be made by our office.

Treatment: We will use and disclose your protected health information to provide, coordinate or manage your health care and any related services. This includes the coordination or management of your health care with a third party. For example, we would disclose your protected health information, as necessary, to a home health agency that provides care to you. We will also disclose protected health information to other physicians who may be treating you. For example, your protected health information may be provided to a physician to whom you have been referred to ensure that the physician has the necessary information to diagnose or treat you.

In addition, we may disclose your protected health information from time to time to another physician or health care provider (e.g., a specialist or laboratory) who, at the request of your physician, becomes involved in your care by providing assistance with your health care diagnosis or treatment to your physician.

Payment: Your protected health information will be used, as needed, to obtain payment for your health care services. This may include certain activities that your health insurance plan may undertake before it approves or pays for the health care services we recommend for you, such as: making a determination of eligibility or coverage for insurance benefits, reviewing services provided to you for protected health necessity, and undertaking utilization review activities. For example, obtaining approval for a hospital stay may require that your relevant protected health information be disclosed to the health plan to obtain approval for the hospital admission.

Health Care Operations: We may use or disclose, as needed, your protected health information in order to conduct certain business and operational activities. These activities include, but are not limited

to, quality assessment activities, employee review activities, training of students, licensing, and conducting or arranging for other business activities.

For example, we may use a sign-in sheet at the registration desk where you will be asked to sign your name. We may also call you by name in the waiting room when your doctor is ready to see you. We may use or disclose your protected health information, as necessary, to contact you by telephone or mail to remind you of your appointment.

We will share your protected health information with third party "business associates" that perform various activities (e.g., billing, transcription services) for the practice. Whenever an arrangement between our office and a business associate involves the use or disclosure of your protected health information, we will have a written contract that contains terms that will protect the privacy of your protected health information.

Sale of Health Information: We will not sell or exchange your health information for any type of financial remuneration without your written authorization.

Fundraising Communications: We may use or disclose your health information for fundraising purposes, but you have the right to opt-out from receiving these communications.

Uses and Disclosures Based On Your Written Authorization: Other uses and disclosures of your protected health information will be made only with your authorization, unless otherwise permitted or required by law as described below.

You may give us written authorization to use your protected health information or to disclose it to anyone for any purpose. If you give us an authorization, you may revoke it in writing at any time. Your revocation will not affect any use or disclosures permitted by your authorization while it was in effect. Without your written authorization, we will not disclose your health care information except as described in this notice.

Others Involved in Your Health Care: Unless you object, we may disclose to a member of your family, a relative, a close friend or any other person you identify, your protected health information that directly relates to that person's involvement in your health care. If you are unable to agree or object to such a disclosure, we may disclose such information as necessary if we determine that it is in your best interest based on our professional judgment. We may use or disclose protected health information to notify or assist in notifying a family member, personal representative or any other person that is responsible for your care of your location, general condition or death.

Marketing: We may use your protected health information to contact you with information about treatment alternatives that may be of interest to you. We may disclose your protected health information to a business associate to assist us in these activities. If we are paid by a third party to make marketing communications to you about their products or services, we will not make such communications to you without your written authorization. Except as stated above, no other marketing communications will be sent to you without your authorization.

Research; Death; Organ Donation: We may use or disclose your protected health information for research purposes in limited circumstances. We may disclose the protected health information of a deceased person to a coroner, protected health examiner, funeral director or organ procurement organization for certain purposes.

Public Health and Safety: We may disclose your protected health information to the extent necessary to avert a serious and imminent threat to your health or safety, or the health or safety of others. We may disclose your protected health information to a government agency authorized to oversee the health care system or government programs or its contractors, and to public health authorities for public health purposes.

Health Oversight: We may disclose protected health information to a health oversight agency for activities authorized by law, such as audits, investigations and inspections. Oversight agencies seeking this information include government agencies that oversee the health care system, government benefit programs, other government regulatory programs and civil rights laws.

Abuse or Neglect: We may disclose your protected health information to a public health authority that is authorized by law to receive reports of child abuse or neglect. In addition, we may disclose your protected health information if we believe that you have been a victim of abuse, neglect or domestic violence to the governmental entity or agency authorized to receive such information. In this case, the disclosure will be made consistent with the requirements of applicable federal and state laws.

Food and Drug Administration: We may disclose your protected health information to a person or company required by the Food and Drug

Administration to report adverse events, product defects or problems, biologic product deviations, to track products; to enable product recalls; to make repairs or replacements; or to conduct post marketing surveillance, as required.

Criminal Activity: Consistent with applicable federal and state laws, we may disclose your protected health information, if we believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. We may also disclose protected health information if it is necessary for law enforcement authorities to identify or apprehend an individual.

Required by Law: We may use or disclose your protected health information when we are required to do so by law. For example, we must disclose your protected health information to the U.S. Department of Health and Human Services upon request for purposes of determining whether we are in compliance with federal privacy laws. We may disclose your protected health information when authorized by workers' compensation or similar laws.

Process and Proceedings: We may disclose your protected health information in response to a court or administrative order, subpoena, discovery request or other lawful process, under certain circumstances. Under limited circumstances, such as a court order, warrant or grand jury subpoena, we may disclose your protected health information to law enforcement officials.

Law Enforcement: We may disclose limited information to a law enforcement official concerning the protected health information of a suspect, fugitive, material witness, crime victim or missing person. We may disclose the protected health information of an inmate or other person in lawful custody to a law enforcement official or correctional institution under certain circumstances. We may disclose protected health information where necessary to assist law enforcement officials to capture an individual who has admitted to participation in a crime or has escaped from lawful custody.

Patient Rights

Access: You have the right to look at or get copies of your protected health information, with limited exceptions. You must make a request in writing to the contact person listed herein to obtain access to your protected health information. You may also request access by sending us a letter to the address at the end of this notice. If you request copies, we will charge you **25¢** for each page, **$15.00** per hour for staff time to locate and copy your protected health information, and postage if you want the copies mailed to you. If the Practice keeps your health information in electronic form, you may request that we send it to you or another party in electronic form. If you prefer, we will prepare a summary or an explanation of your protected health information for a fee. Contact us using the information listed at the end of this notice for a full explanation of our fee structure.

Accounting of Disclosures: You have the right to receive a list of instances in which we or our business associates disclosed your non-electronic protected health information for purposes other than treatment, payment, health care operations and certain other activities during the past six (6) years. For disclosures of electronic health information, our duty to provide an accounting only covers disclosures after January 1, 2011 [January 1, 2014] and only applies to disclosures for the three (3) years preceding your request. We will provide you with the date on which we made the disclosure, the name of the person or entity to whom we disclosed your protected health information, a description of the protected health information we disclosed, the reason for the disclosure, and certain other information. If you request this list more than once in a 12-month period, we may charge you a reasonable, cost-based fee for responding to these additional requests. Contact us using the information listed at the end of this notice for a full explanation of our fee structure.

Restriction Requests: You have the right to request that we place additional restrictions on our use or disclosure of your protected health information. Except as noted herein, we are not required to agree to these additional restrictions, but if we do, we will abide by our agreement (except in an emergency). We are required to accept and follow requests for restrictions of health information to insurance companies if you have paid out-of-pocket and in full for the item or service we provide to you. Any agreement we may make to a request for additional restrictions must be in writing signed by a person authorized to make such an agreement on our behalf. We will not be bound unless our agreement is so memorialized in writing.

Confidential Communication: You have the right to request that we communicate with you in confidence about your protected health information by alternative means or to an alternative location. You must make your request in writing. We must accommodate your request if it is reasonable, specifies

the alternative means or location, and continues to permit us to bill and collect payment from you.

Amendment: You have the right to request that we amend your protected health information. Your request must be in writing, and it must explain why the information should be amended. We may deny your request if we did not create the information you want amended or for certain other reasons. If we deny your request, we will provide you a written explanation. You may respond with a statement of disagreement to be appended to the information you wanted amended. If we accept your request to amend the information, we will make reasonable efforts to inform others, including people or entities you name, of the amendment and to include the changes in any future disclosures of that information.

Electronic Notice: If you receive this notice on our website or by electronic mail (e-mail), you are entitled to receive this notice in written form. Please contact us using the information listed at the end of this notice to obtain this notice in written form.

Notice of Unauthorized Disclosures: If the Practice causes or allows your health information to be disclosed to an unauthorized person, the Practice will notify you of this and help you mitigate the effects.

Questions and Complaints

If you want more information about our privacy practices or have questions or concerns, please contact us using the information below.

If you believe that we may have violated your privacy rights, or you disagree with a decision we made about access to your protected health information or in response to a request you made, you may complain to us using the contact information below. You also may submit a written complaint to the U.S. Department of Health and Human Services. We will provide you with the address to file your complaint with the U.S. Department of Health and Human Services upon request.

We support your right to protect the privacy of your protected health information. We will not retaliate in any way if you choose to file a complaint with us or with the U.S. Department of Health and Human Services.

Name of Contact Person: Angie Buehler

Telephone: **(801) 313-4112** Email: abuehler@spradiology.com

Address: **5444 South Green Street, Murray, UT 84123**

ACKNOWLEDGMENT OF RECEIPT
OF
NOTICE OF PRIVACY PRACTICES

I acknowledge that I was provided a copy of the Notice of Privacy Practices and that I have read (or had the opportunity to read if I so chose) and understood the Notice.

_____ _____
Patient Name (please print) Date

_____
Parent or Authorized Representative (if applicable)

_____
Signature

APPENDIX B

Sample Business Associate Agreement

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (Agreement) is made and entered into by and between Summit Physician Specialists, PC, and _____ **[insert name of Business Associate]** on this _____ day of _____, 20___. In consideration of the mutual covenants contained in this Agreement and intending to be legally bound, the parties agree as follows:

1. Definitions:

Business Associate. "Business Associate" shall mean _____ **[Insert Name of Business Associate]**.

ePHI. "ePHI" shall mean Protected Health Information transmitted by or maintained in electronic media.

Practice. The "Practice" shall mean Summit Physician Specialists, PC**.**

Patient. "Patient" shall have the same meaning as the term "individual" in 45 CFR 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.

Protected Health Information. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR 164.501, as limited to the information created or received by Business Associate from or on behalf of Practice.

Required By Law. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR 164.501.

Secretary. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his/her designee.

Security Incident. "Security Incident" shall mean a violation of the Security Rule, or the breach of confidentiality, integrity or accessibility of ePHI.

Security Rule. "Security Rule" shall mean the statutes for security of individually identifiable health information at 45 CFR part 164, subpart C.

Unsecured Protected Health Information. Protected Health Information that has not been rendered unusable, unreadable or indecipherable to unauthorized individuals.

2. Obligations and Activities of Business Associate

Business Associate agrees:

(a) Not to use or disclose Protected Health Information other than as permitted or required by this Agreement and the HIPAA Privacy Rule.

(b) To use appropriate administrative, physical and technical safeguards to prevent use or disclosure of the Protected Health Information and ePHI as specified by the HIPAA Privacy and HIPAA Security Rules.

(c) To mitigate, to the extent practicable, any harmful effect that is known to Business Associate as a result of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

(d) To report to Practice any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.

(e) To ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Practice, agrees, in writing, to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

(f) To provide access, at the request of Practice, and in the time and manner requested by the Practice, to Protected Health Information to the Practice or, as directed by Practice, to Patient in order to meet the requirements under 45 CFR 164.524. Such access may include access to, and copies of, Protected Health Information maintained by Business Associate in electronic form.

(g) To make any amendment(s) to Protected Health Information in a Designated Record Set that the Practice directs or agrees to pursuant to 45 CFR 164.526 at the request of Practice or a Patient, and in the time and manner requested by the Practice.

(h) To disclose only the minimum necessary Protected Health Information when disclosure must be made. Whenever possible, Business Associate will redact or delete the following items from the Protected Health Information disclosed to others:

- Names;
- Postal address information, other than town or city, state, and zip code;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social Security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints; and
- Full face photographic images and any comparable images;

(i) Not to sell Protected Health Information that it receives from the Practice to any other person or entity.

(j) To make its internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of Practice available to the Practice, or to the Secretary, in a time and manner requested by the Practice or designated by the Secretary, for purposes of the Secretary determining Practice's compliance with the Privacy Rule and Security Rule.

(k) To document all disclosures of Protected Health Information and information related to such disclosures as would be required for Practice to respond to a request by a Patient for an accounting of disclosures of Protected Health Information in accordance with federal and state laws and regulations.

(l) To report to Practice any security incident or breach of protected health information of which it becomes aware.

(m) To authorize termination of the Agreement by Practice, if Practice determines that the Business Associate has violated a material term of the contract.

(n) To give notice to a Patient, in the form and manner directed by the Practice, if Business Associate causes or allows an unauthorized disclosure of unsecured Protected Health Information.

(o) To follow, to the extent possible, the guidelines published by the Secretary relating to the technology for rendering electronic Protected Health Information unusable, unreadable or indecipherable to unauthorized individuals.

3. Permitted Uses and Disclosures by Business Associate

[use one of the following versions]

Specific purposes: Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, Practice for the following purposes, if such use or disclosure of Protected Health Information would not violate the Privacy Rule or Security Rule if done by Practice or the minimum necessary policies and procedures of the Practice: _____ _____ _____ **[List Purposes]**.

<or>

Underlying services agreement: Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities or services for, or on behalf of, Practice as specified in the agreement with _____ **[Insert Name of Business Associate]**, provided that such use or disclosure would not violate the Privacy Rule or Security Rule if done by Practice or the minimum necessary policies and procedures of the Practice.

4. Obligations of the Practice

Practice shall:

(a) Notify Business Associate of any limitation(s) in its notice of privacy practices of Practice in accordance with 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.

(b) Notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

(c) Notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Practice has agreed to in accordance with 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

5. Permissible Requests by Practice

Practice shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule or Security Rule if done by Practice.

6. Term and Termination

(a) Term: This Agreement shall be effective as of _____ **[Insert Effective Date]**, and shall terminate when all of the Protected Health Information provided by Practice to Business Associate, or created or received by Business Associate on behalf of Practice, is destroyed or returned to Practice, or, if it is impractical to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.

(b) Termination for Cause: Upon Practice's knowledge of a material breach by Business Associate, Practice shall either: (1) Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement and any related agreement if Business Associate does not cure the breach or end the violation within the time specified by Practice; (2) Immediately terminate this Agreement and any related agreement entered into by the parties if Business Associate has breached a material term of this Agreement and cure is not possible; or (3) If neither termination nor cure are feasible, Practice shall report the violation to the Secretary.

(c) Effect of Termination:

(1) Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Practice, or created or received by Business Associate on behalf of Practice. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

(2) In the event that Business Associate determines that returning or destroying the Protected Health Information is impractical, Business Associate shall provide to Practice notification of the conditions that make return or destruction impractical. Upon providing notice that return or destruction of Protected Health Information is impractical, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction impractical, for so long as Business Associate maintains such Protected Health Information.

7. Miscellaneous

(a) Regulatory References: A reference in this Agreement to a section in the Privacy Rule or Security Rule means the section as in effect or as amended.

(b) Amendment: The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Practice to comply with the requirements of the HIPAA Privacy Rule or Security Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

(c) Survival: The respective rights and obligations of Business Associate under subsection 4(c) of this Agreement shall survive the termination of this Agreement.

(d) Interpretation: Any ambiguity in this Agreement shall be resolved to permit Practice to comply with the HIPAA Privacy Rule or Security Rule.

8. Indemnification

Business Associate shall defend and indemnify the Practice from and for any and all liability, claims, proceedings, suits, damages, or causes of action resulting in any way from Business Associate's breach of this Agreement or breach of the HIPAA Privacy Rule or HIPAA Security Rule. The duty to indemnify shall include the duty to defend the Practice by hiring competent legal counsel at Business Associate's expense.

The parties have caused this Agreement to be executed on the date first written above.

Summit Physician Specialists, PC	**[Insert name of Business Associate]**
By:_____	By:_____
Its:_____	Its:_____

APPENDIX C

Patient Authorization to Release Health Information

Summit Physician Specialists, PC
5444 South Green Street
Murray, UT 84123

AUTHORIZATION FOR RELEASE OF INFORMATION

I hereby authorize Summit Physician Specialists, PC, to disclose my protected health information as described below. I understand that this authorization is voluntary. I understand that the information disclosed pursuant to this authorization may be subject to redisclosure by the recipient and may no longer be protected by federal or state law. I understand that I may see and copy the information described on this form if I ask for it, and that I will receive a copy of this form after I sign it. I understand that I may revoke this authorization at any time by giving notice in writing at the address found above, but if I do it will not affect any actions taken before receipt of my revocation.

I understand that my treatment will not be conditioned on whether I provide authorization for the requested use or disclosure except (1) if my treatment is related to research, or (2) health care services are provided to me solely for the purpose of creating protected health information for disclosure to a third party.

Patient name:_____ **Date of birth:**_____
Persons/organizations to receive the information: _____

The specific information to be released/disclosed is specified below:

☐ **Complete Medical Record**
Or specify one or more of the following:

☐	Operative Reports	☐	X-rays
☐	Progress Notes	☐	Billing and Claim Records
☐	Laboratory	☐	(Other – specify) _____

This information is to be used/disclosed for the following purposes(s) only: _____
_____
(no purpose need be stated if the request is made by the patient and the patient does not wish to state the purpose).

This authorization will expire on _____ (state date or event).

SPECIFIC AUTHORIZATION

I understand that my health information to be released MAY INCLUDE information that is related to sexually transmitted disease, acquired immunodeficiency syndrome (AIDS), or human immunodeficiency virus (HIV), behavioral or mental health services, and/or treatment for alcohol and/or drug abuse. My signature below authorizes release of all such information, unless I have crossed it out, and initialed it.

☐ **Yes** ☐ **No** _____**Initials**

_____ _____
Signature of patient or patient's representative **Date**
(Form MUST be completed before signing.)

Printed name of patient's representative (if applicable):_____
Relationship to the patient (if applicable):_____

*** YOU ARE ENTITLED TO A COPY OF THIS DOCUMENT**

APPENDIX D

Practice Resolutions

PRACTICE RESOLUTION
ADOPTION OF HIPAA PRIVACY MANUAL

WHEREAS, Summit Physician Specialists, PC, has authorized the creation of a HIPAA Privacy Manual; and

WHEREAS, the Practice has reviewed the Privacy Manual; and

WHEREAS, the Privacy Manual is intended to satisfy fully the requirements set forth in the federal HIPAA Privacy Rules;

NOW THEREFORE,

BE IT RESOLVED, that the Practice hereby approves of the adoption of the HIPAA Privacy Manual, effective March 1, 2020, with the expectation that all Practice employees, including those with an ownership interest in the Practice, will be instructed in their respective duties under the Manual and will comply fully therewith.

Date:_____

By:_____

PRACTICE RESOLUTION
APPOINTMENT OF A PRIVACY OFFICER

WHEREAS, Summit Physician Specialists, PC ("the Practice"), having approved the adoption of the HIPAA Privacy Manual; and

WHEREAS, the Privacy Manual requires the appointment of a Privacy Officer; and

WHEREAS, the Practice having great confidence in the integrity, experience, and judgment of Angie Buehler;

NOW THEREFORE,

BE IT RESOLVED, that the Practice does hereby appoint Angie Buehler to be the Privacy Officer of the Practice beginning March 1, 2020, and continuing until changed in accordance with the HIPAA Privacy Manual; and

BE IT FURTHER RESOLVED, that the Privacy Officer will vigorously carry out the duties set forth in the Privacy Manual and that all employees of the Practice will be informed of the importance of adherence to the Privacy Manual and the importance of their cooperation with the Privacy Officer.

Date:_____

By:_____

APPENDIX E

Privacy Training and Education Log

PRIVACY TRAINING AND EDUCATION LOG

Date of Training	Name of Employee	Description of Training	Training Hours	Person/Company Providing Training

APPENDIX F

Patient Complaint Form

PATIENT COMPLAINT FORM

Patient Name:

Name of person submitting this complaint (if other than patient):

Relationship to Patient:

Please provide the following information regarding your complaint:

Date the conduct complained of occurred:

Practice personnel involved in this matter:

Complete details and description of the reason for your complaint:

What can our office do to address your complaint?

Signature

Date

For Practice Use Only

Description of Action Taken to Address Patient Complaint: Privacy Officer Signature: Date:

APPENDIX G

Accounting of Disclosures Forms

ACCOUNTING OF DISCLOSURES OF NON-ELECTRONIC HEALTH INFORMATION

Pursuant to your written request for an accounting of the disclosures made by the Practice of your non-electronic protected health information, the following are the disclosures made during the past six (6) years which the Practice is required to track and account for under the HIPAA Privacy Rules:

Date of Disclosure	Person/Entity to Whom Disclosures Were Made	Record of Information Disclosed	Reason for the Disclosure

Note: Under the federal HIPAA Privacy Rules, the Practice is not required to track and account for disclosures of non-electronic health information:

- For purposes of treatment, payment activities or health care operations (see definition in Glossary, Appendix H);
- To the patient;
- Pursuant to an authorization signed by the patient;
- To correctional institutions or law enforcement officers; or
- That occurred prior to April 14, 2003.

Accordingly, the accounting provided herein does not include the above categories or types of disclosures.

Privacy Officer Signature:

Date:

ACCOUNTING OF DISCLOSURES OF ELECTRONIC HEALTH INFORMATION

Pursuant to your written request, the Practice provides the following accounting of disclosure of electronic health information which occurred in the past three (3) years:

Date of Disclosure	Person/Entity to Whom Disclosures Were Made	Record of Information Disclosed	Reason for the Disclosure

Note: Under the federal law, the Practice is not required to account for disclosures of electronic health information that occurred prior to January 1, 2011 [January 1, 2014, if the Practice maintained the electronic information prior to January 1, 2009].

Privacy Officer Signature:

Date:

APPENDIX H

Glossary of Terms

GLOSSARY OF TERMS

Authorization – Written permission granted by the patient or the patient's guardian to use or disclose protected health information for purposes other than treatment, payment, health care operations or uses and disclosures permitted or required by the HIPAA Privacy Rule.

Business associate – A person or entity who creates, receives, maintains or transmits protected health information on behalf of a covered entity (or of an organized health care arrangement in which the covered entity participates). A business associate may assist in the performance of:

- A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
- Any other function or activity regulated by this subchapter; or
- A person who provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity (or to or for an organized health care arrangement in which the covered entity participates) where the provision of the service involves the disclosure of individually identifiable health information from such covered entity (or arrangement), or from another business associate of such covered entity (or arrangement), to the person.
- Subcontractor of business associates are also classified as business associates.

Contact person – The individual designated by a health care provider to (1) receive patient complaints regarding privacy matters and (2) provide further information about topics covered in the Notice of Privacy Practices.

Covered entity – (1) A health plan (includes insurance companies, Medicare, Medicaid, group health plans, etc.); (2) a health care clearinghouse; or (3) a health care provider who transmits any health information in electronic form in connection with a standard HIPAA transaction (such as electronic billing).

Designated record set – A group of records maintained by or for a covered entity that includes the protected health records and billing records about individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication, and case or protected health management record systems maintained by or for a health plan; or used, in whole or in part, by or for the covered entity to make decisions about individuals. For purposes of this definition, the term *record* means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

Disclosure – Any release, transfer, provision of access to, or divulging in any other manner of protected health information outside the entity holding the information.

HHS or Secretary – The Department of Health and Human Services or the Secretary of Health and Human Services.

Health care – Care, services, or supplies related to the health of an individual. *Health care* includes, but is not limited to, the following:

(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and

(2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health care operations – Any of the following activities of the covered entity to the extent that the activities are related to covered functions, and any of the following activities of an organized health care arrangement in which the covered entity participates:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

(3) Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;

(4) Conducting or arranging for protected health review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

(6) Business management and general administrative activities of the entity, including, but not limited to:

(i) Management activities relating to implementation of and compliance with the requirements of this subchapter;

(ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.

(iii) Resolution of internal grievances;

(iv) Due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a covered entity or, following completion of the sale or transfer, will become a covered entity; and

(v) Consistent with the applicable requirements of § 164.514, creating de- identified health information, fundraising for the benefit of the covered entity, and marketing for which an individual authorization is not required as described in § 164.514(e)(2).

Health care provider – A provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of protected health or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health information – Any information, oral or recorded in any medium, that:

- Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Individually identifiable health information – Information that is a subset of health information, including demographic information collected from an individual, and that: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (i) Which identifies the individual, or (ii) With respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

IRB - Institutional Review Board, established to review research activities in accordance with federal regulations.

Law enforcement official – An officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

(1) Investigate or conduct an official inquiry into a potential violation of law; or

(2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Marketing –

(1) To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service, unless the communication is made:

(i) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.

(ii) For treatment of the individual; or

(iii) For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

(2) An arrangement between a covered entity and any other entity whereby the covered entity discloses PHI to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

Minimum necessary – When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

Payment – Any of a number of activities by a covered entity involving reimbursement or coverage related to health care or health benefits. The definition of payment includes: obtaining premiums or identifying or providing benefits under a health plan; reimbursement for health services, determining eligibility, coverage, adjudication, or subrogation of health benefit claims; risk adjusting amounts due based on enrollee health status and demographics; billing, claims management, collection activities, obtaining payment under a contract for reinsurance and related health care data processing; review of health care services for protected health necessity,

coverage under a health plan, appropriateness of care, or justification of charges; utilization review activities, including pre-certification and preauthorization of services, concurrent and retrospective review of services; and disclosure to consumer reporting agencies of certain protected health information relating to collection of premiums or reimbursement (i.e., 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).

Privacy officer – The individual designated by a health care provider to develop and implement privacy policies and procedures for the provider.

Protected health information – Individually identifiable health information that is or has been electronically maintained or electronically transmitted by a covered entity, as well as such information when it takes any other form that is (1) Created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

Public health authority – An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Required by law – A mandate contained in law that compels a covered entity to make a use or disclosure of protected health information and that is enforceable in a court of law. *Required by law* includes, but is not limited to, court orders and court- ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

Research – Means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Treatment – The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Use – Means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Workforce – Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

APPENDIX I

HIPAA Resources

HIPAA RESOURCES

Helpful General and Government Websites

Listed below are some valuable resources on the Internet that provide general information about HIPAA:

- Accredited Standards Committee – X12N: http://www.x12.org
- American Health Information Management Association: http://www.ahima.org
- CMS HIPAA Site: http://www.cms.hhs.gov/hipaa/hipaa2/default.asp
- CMS's Links to other Administrative Simplifications Sites: http://www.hcfa.gov/medicare/edi/hipaaedi.htm
- HIPAAlert: http://www.hipaalert.com
- Institute for Health Care Research and Policy, Georgetown University http://www.healthprivacy.org
- Phoenix Health System: http://www.hipaadvisory.com
- SNIP: http://snip.wedi.org
- WEDI: http://www.wedi.org

APPENDIX J

Request for Correction/Amendment of Health Information

REQUEST FOR CORRECTION/AMENDMENT OF HEALTH INFORMATION

Patient Name:

Birth Date:

Patient Address:

Patient
Phone Number:

Date of entry to be amended:

Type of entry to be amended:

Please explain how the entry is incorrect or incomplete. What should the entry say to be more accurate or complete? Please use additional paper, if necessary.

Would you like the amendment sent to anyone to whom we may have disclosed the information in the past? If so, please specify the name and address of the organization or individual.

Name

Address

Name

Address

Signature of Patient or Legal Representative

Date

For Practice Use Only:

Date Received

Amendment has been: ☐ Accepted ☐ Denied

If denied, check reason for denial:

☐ PHI is not available to the patient for inspection as required by federal law (e.g., psychotherapy notes)

☐ PHI was not created by the Practice

☐ PHI is not part of patient's designated record set

☐ PHI is accurate and complete

Comments of Health Care Practitioner:

Name of Staff Member

Title

Signature of Health Care Practitioner

Date

APPENDIX K

Restriction Request Form

RESTRICTION REQUEST FORM

For Use and Disclosure of Patient Health Information

In completing this form, you are requesting that the following restrictions be considered as limitations to the use and disclosure of your protected health information. If we grant your request, we are bound by the terms of the agreement. You will be notified in writing of Summit Physician Specialists, PC's decision to accept or deny your restriction request. Until a decision is reached, your request for restriction will not be honored.

Requested Restrictions (please provide specific details and dates):

Print Patient Name:

Signature of Patient or Authorized Representative:

Date:

Relationship to Patient:

For Practice Use Only:

Practice:	☐ Accepts	☐ Denies
Privacy Officer Signature:		
Date:		

Note: The Practice must honor requests for restrictions of health information by the patient if (1) the disclosure will be to an insurance company for purposes of payment or health care operations, and (2) the patient has paid for the service out of pocket in full.

APPENDIX L

Request for Confidential Communications

REQUEST FOR CONFIDENTIAL COMMUNICATIONS

Name of Patient:

(please print)

Date of Birth:

I request that all communications to me (by telephone, mail or otherwise) by Summit Physician Specialists, PC, and/or its staff be handled in the following manner:

- For written communications: Address to:

_____

- For oral communications: Call:

(telephone number)

May we leave a message?

Yes ☐

No ☐

If the address provided above is not your home address or is not a street address, please provide us with a street address for purposes of ensuring payment:

_____

_____

Patient Signature

Date

For Practice Use Only

Practice:	☐	Accepts
☐	Denies	

Privacy Officer Signature:

Date:

APPENDIX M

Quick Reference Regarding Disclosures Requiring/Not Requiring Written Patient Authorization

Quick Reference: Disclosures Requiring/Not Requiring Written Patient Authorization

Disclosures Not Requiring Written Patient Authorization:

- To the patient himself/herself (Manual, Section C.1.1.1).
- To other persons/entities for purposes of the Practice's treatment, payment or health care operations (Manual, Section C.1.1.2).
- To another health care provider for that provider's treatment of the patient (Manual, Section C.1.1.3).
- To other health care providers or HIPAA "covered entities" for purposes of their making/obtaining payment for health care services (Manual, Section C.1.1.4).
- To a HIPAA "covered entity" for purposes of its health care operations (Manual, Section C.1.1.5).
- To parents of minors, guardians, conservators or other authorized representatives of the patient (Manual, Section C.2).
- To family members and/or caregivers where patient does not object verbally or where disclosure is indicated by the provider's professional judgment (Manual, Section C.3).
- To government authorities as required by law (Manual, Section C.4):
    - public health reporting
    - child abuse/other abuse
    - domestic violence
    - health oversight activities (audits, investigations)
    - court orders, subpoenas, search warrants
    - law enforcement (under certain circumstances)
- To government authorities or potential victims to prevent serious harm or injury (Manual, Section C.5).
- To business associates pursuant to a proper business associate agreement (Manual, Section C.6).
- For certain "research" activities (Manual, Section C.7).
- For certain "marketing" activities (Manual, Section C.7).

Disclosures Requiring Written Patient Authorization

- All other disclosures of patient health information (Manual, Section B.2).

APPENDIX N

Acknowledgment of Receipt/Review of HIPAA Privacy Manual

ACKNOWLEDGMENT OF RECEIPT/REVIEW
OF
HIPAA PRIVACY MANUAL

I, _____, acknowledge that I have received and/or reviewed
(print full name)
the Practice's HIPAA Privacy Manual and that I will comply with its provisions. I acknowledge that failure to comply could result in disciplinary action, up to and including termination.

_____ _____
(Signature) (Date)