

HIPAA Privacy and Confidentiality Policies for the
University of Nevada School of Medicine Multi-specialty
Group Practice South, Inc. dba MedSchool Associates
South



*Established by and is effective on April 14, 2003
University of Nevada School of Medicine
Multi-specialty Group Practice South, Inc.
2040 West Charleston Blvd. #400
Las Vegas, NV 89102*

*Form#HP003
Rev. 3/13/03
Rev. 4/6/06*

Table of Contents-Privacy manual

<u>Policy numbers</u>	<u>Page Number</u>
HIPAA Privacy Policy Manual-overview	2
1.0 Privacy and Policy statement	3
2.0 Rules Pertaining to Staff	3-4
3.0 HIPAA-safe privacy management software	5
4.0 Complex entity	5
5.0 Designated Record Set	6
6.0 Notice of Privacy Practices policy	7-8
7.0 Privacy Officer	9
8.0 HIPAA committee	10
9.0 Sending PHI to another entity	11-12
10.0 Requests for PHI	13-14
11.0 Denial of disclosure policy	15
12.0 Retention and security of records	16
13.0 Intake process-sign in sheet	16-17
14.0 Discipline of employees	17
15.0 Disclosure of PHI	17-18
16.0 Types of uses and disclosures w/o auth	18-19
17.0 Other uses and disclosures w/o auth	19-23
18.0 Minimum Necessary information	23
19.0 Amendment to medical record policy	23-24
20.0 Disclosure Accounting policy	24
21.0 Request to restrict disclosure of PHI	24
22.0 Alternative communications	24-25
23.0 Documentation of privacy activities policy	25
24.0 Initial Privacy assessment	25
25.0 Complaint manager policy	25
26.0 Appeals process policy	25-26
27.0 Employee acknowledgement form	27

HIPAA Privacy Policy Manual

Overview

This manual is written to comply with the Health Insurance Portability and Accountability Act of 1996 referred to as HIPAA. This law was passed to promote more standardization and efficiency in the health care industry. There are four parts to HIPAA's Administrative Simplification:

- 1) Privacy requirements
- 2) Electronic Transaction and Code Sets Standards requirements
- 3) Security requirements
- 4) National Physician Identifier requirements

This manual is designed to be a "work in process" and will be divided into 4 separate parts. The first section will focus on policies for MedSchool Associates South for privacy compliance. The next section will be written to address policies associated with implementation of electronic transactions and code sets. The security requirements will be the third section and these rules have just been finalized. The plan for implementation will be developed as soon as the security rules are published. The final section will be designed for policies applicable to the National Physician Identifier requirements which have not yet been finalized.

MedSchool Associates South is committed to following all federal and state laws and regulations in regard to the above mentioned policies. All physicians, residents, medical students, staff, employees, independent contractors, and volunteers will be trained on the policies and procedures in this manual. Annually, all above mentioned personnel will be required to sign an oath of confidentiality to maintain the privacy of patient information. Additionally, all personnel will need to certify in writing that they have received, read, received training on, understand and agree to follow the policies in this manual. Any violations of these policies may lead to termination of employment with MedSchool Associates South or the University of Nevada School of Medicine and/or could result in expulsion of academic programs. All certifications will be kept in the Privacy Officer's office. For new hire personnel, these certifications will be signed within a reasonable amount of time after hire.

The following privacy policies have been adopted and shall be used as a basis for our clinics and offices in handling, protecting and disclosing Protected Health Information (PHI). We request all current employees to acknowledge receipt of these privacy policies and certify in writing that they have read, will follow the policies and report any unauthorized disclosures of PHI to the Privacy Officer. These certifications are tracked through the Privacy Management Software Program HIPAA-safe. Additionally, adherence to these policies will become part of the annual employee review process and has been added to their job descriptions. These documents will be kept in their personnel file.

Section 1.0-Privacy and Policy Statement

The United States Department of Health and Human Services has adopted certain regulations governing the privacy of protected health information pursuant to the Health Insurance Portability and Accountability Act of 1996. (“HIPAA”). These new regulations are known as the “HIPAA Privacy Rule”. In addition, state law may impose restrictions on the use or disclosure of patient health information that are more stringent than federal regulations. It is our objective to maintain adequate procedures and security to meet state and federal requirements governing protected patient health information in order to ensure the integrity and confidentiality of the information, to protect against any reasonably anticipated threats to the security of the information and to guard against unauthorized uses or disclosures of the information.

Protected Health Information (or “PHI”) has a specific meaning under the HIPAA Privacy Rule. Basically, PHI refers to any individually identifiable health information related to current or former patients. PHI includes identifying information such as a patient’s name, age, address, telephone number, social security number, marital status and the like, as well as the patient’s health history, treatment records, financial information and any other information related to the patient when this information can be used to identify the patient.

The privacy of patient information is very important to our patients and our offices. It is important that we reasonably protect the patient’s health information in a way that helps keep the information within our facilities yet allows our business to operate reasonably and efficiently so we may provide high-quality service to our clients. To that end, we adopt the following policies and will follow the policies to help ensure that our offices do not improperly use and/or disclose protected information.

Section 2.0- Rules Pertaining to Staff

A. Applicability

These policies and procedures apply to all of our administrators, employees, staff, volunteers, residents, medical students, physician faculty, temporary employees, externs, interns, and high school students, as well as other employees of the University of Nevada School of Medicine and MedSchool Associates South who assist us in various health care operations requiring access to PHI in our possession such as accountants, auditors, attorneys, disbursement offices and information technology officials. These policies and procedures also apply to our business associates to whom we disclose PHI. Business associates are outside companies or individuals that perform a service for us that require the company or individual to receive PHI.

B. Privacy and Security Officers

We have designated a Privacy Officer who is responsible for the implementation of federal and state privacy laws. In addition, the Privacy Officer is responsible to review complaints and answer questions about privacy policies and procedures. We have also designated a Security Officer. A Security Officer is responsible for ensuring we take reasonable efforts to protect the storage and transmission of health information by electronic means. Further discussion related to the Privacy Officer is found later in this manual.

C. Employee Designations for Security Purposes

We will evaluate personnel and job descriptions to identify which employees need access to PHI and whether that access should be limited in some manner. Employees will be advised as to the appropriate level of access they have to PHI. This level of access could range from no access to complete access. We have modified employee job descriptions to reflect these limitations. In addition, keys to offices and storage cabinets in which PHI is stored have been appropriately limited and password protection has been established to ensure privacy of PHI.

D. Employee Training

All existing employees have been trained, with respect to HIPAA and our policies and procedures by April 14, 2003. All new employees will receive HIPAA training at, or shortly after, their hire date through new hire orientation within 30 days. From time to time additional training will be provided as necessary to address changes in policies and procedures, as well as changes in the law. The Privacy Officer and/or Supervisors should document the training provided and the individuals in attendance. A copy of any training materials will be retained.

E. Privacy Violations

There are severe penalties under HIPAA for wrongfully disclosing or using health information in a manner. These penalties could include significant civil fines, and even criminal penalties, particularly for knowing violations for gain (e.g. an employee takes money from a third party in exchange for release of PHI).

All employees, volunteers and trainees have signed a letter of instruction prior to April 14, 2003, and at least every three years thereafter, which affirms the commitment to abide by federal and state privacy laws. (For students/trainees, the violation of the law and/or our policies and procedures could result in discipline, up to and including termination or expulsion from the program for the first offense.) For employees, violation of the law and/or our policies and procedures could result in discipline, up to and including termination from employment for the first offense. Discipline will be taken in accordance with any required disciplinary procedures.

Section 3.0 – Enterprise Compliance Management Software System

Our office has purchased a privacy management software tool named, Enterprise Compliance Manager (ECM), to assist in the tracking of our employee education, and to manage the disclosures required by law of our patients' PHI. All employees who will use the software tool will be trained on the use of the software and be responsible for all required entries into the system. The Privacy Officer will manage the overall activity of the ECM program and will ensure that the software is used appropriately.

Section 4.0 Complex Entity

The University of Nevada School of Medicine is a hybrid covered entity in an organized healthcare arrangement with the University of Nevada School of Medicine Multi-specialty Group Practice South Inc. dba MedSchool Associates South. The School has a complex diverse operation plan for health care delivery, billing claims processing, clinical, academic and administrative operations.

Hospitals that the School works with include, but are not limited to, University Medical Center including some UMC Quick Care clinics, Sunrise, Mountain View, Valley, Summerlin, Desert Springs, St. Rose Dominican and Siena campus Hospitals, Southern Hills, HealthSouth Rehab Hospitals - multiple locations, VA Hospital, Sahara and Flamingo Surgery Centers, IHS Specialty Hospitals, and North Vista. In addition, MedSchool Associates South Patient Care Center, the NV Tobacco Users' Helpline and a Sunrise OB medical clinic at Fitzgeralds, Family Medicine at Fire Mesa, Surgical clinic at Tenaya and a Surgical clinic at Maryland Parkway are also locations where the School and its employees will practice. Also included is a Pediatric clinic located in the medical building complex next to Sunrise Hospital, Maternal Fetal Medicine, and a separate Alzheimer's clinic in the Reno area, and Maternal Fetal Medicine. The NFPRP Family Practice and Mojave Health Care Clinic, Lili Claire Foundation, the Pediatric Dental Residency and the School's Dental Residency Program at the PCC are also included in this entity. This list is meant to identify most of the locations that are identified to be part of the covered entity under the HIPAA rules and is not meant to be totally inclusive.

The following departments and clinics are not considered covered under the HIPAA regulations:

- Department of Geriatric Education
- Human Resources (Ask Tom Ray)
- Southern Nevada AHEC
- Facilities Management

Section 5.0 -Designated Record Set

A “record” is any item of protected health information that is maintained, collected, used or disseminated by a covered entity.

MedSchool Associates South defines a designated record set to include the patient medical record including lab and radiology results, office visit documentation, operative notes, physician orders, written notes as well as dictated physician notes and may include hospital generated progress notes and records. In addition to the medical record, all patient billing information including a HCFA 1500 form both in paper and electronically, a super-bill and all staff notations that are kept in regard to follow-up on the patient account are included in the designated record set. These documents would include all notations made by outside billing agents contracted with the School as well as internal patient notations in the MISYS system. All collection letters generated by the contracted third party agency are also included as part of the designated record set.

Section 6.0-Policy Regarding the Notice of Privacy Practices

All patients seeking services after April 14, 2003 must receive a copy of our Notice of Privacy Practices prior to obtaining the requested services, in addition to other forms that we require during the intake process. We are required to try to obtain the patient's signature acknowledging receipt of the Notice of Privacy Practices and to keep a copy of this acknowledgment in the patient's medical records. If the patient refuses to sign the acknowledgment of receipt, that should be noted on the acknowledgment and a copy placed in the patient's medical records and an entry made into the ECM privacy management tool.

A patient is entitled to a copy of the Notice of Privacy Practices. We have posted a copy of our Notice of Privacy Practices in the waiting room of each clinic in every department where patients are seen. If a patient has any questions about the Notice of Privacy Practices that cannot be answered clearly from the Notice of Privacy Practices, the patient should be referred to a clinic staff member and if the question is not answered, then the Privacy Officer should be contacted.

Beginning on April 14, 2003 each patient has received a copy of the Notice of Privacy Practices and sign a written affirmation that he/she has received a copy of the Notice. This signed affirmation will be kept in the patient medical record. If the patient requests an additional copy of this notice, one (1) notice will be provided at no charge annually. If additional copies of the notice are requested, then MedSchool Associates South will charge the patient a fee of .60 per page to copy the notice. Using the ECM program, all patient acknowledgements will be documented and tracked.

In certain circumstances, we may treat patients in an emergency situation, or in a situation where the first contact with the patient occurs at a location other than our facility. If that is the case, we will mail a Notice of Privacy Practices to the patient and request a return acknowledgment or we will provide the Notice to the patient in some manner as requested by the patient, such as by email or fax.

In some situations, we may treat individuals who are minors or who are otherwise not capable of consent. In these situations, we will provide the Notice of Privacy Practices to the patient and the patient's representative. We should attempt to obtain the signature of the patient on the acknowledgment, if of sufficient age of understanding, and should also obtain the signature of the guardian, parent or other legal representative acknowledging receipt of the Notice of Privacy Practices.

From time to time we may change our Notice of Privacy Practices. If we change the Notice of Privacy Practices we will apply the changes to all patient information, including health information obtained prior to the change. The change will not be effective until the new Notice of Privacy Practices is posted. All versions of the Notice of Privacy Practices that we have used from time to time should be archived by the Privacy Officer and/or Supervisors.

Existing patients who have already signed a Notice of Privacy Practices are not required to acknowledge receipt of an amended Notice of Privacy Practices. However, the patient is entitled to a copy of the amended Notice of Privacy Practices upon request.

All employees should carefully read the Notice of Privacy Practices and any amendment. The Notice sets forth the rights of the patient with respect to their health information. These rights and our policies pertaining to these rights, are described in further detail in these policies and procedures.

Section 7.0 Privacy Officer

The Privacy Officer has been appointed by the Vice Dean of the School of Medicine. For MedSchool Associates South the Director of Billing Compliance will serve as the Privacy Officer. The Privacy Officer will be the main contact for all employees for questions regarding release of medical information, HIPAA electronic standards and data sets, and patient questions regarding any of our privacy policies and procedures. The Privacy Officer will manage and act as the administrator for the ECM privacy management software tool. All internal privacy forms as well as attestations for employees will be generated by the Privacy Officer. All external requests for Protected Health Information (PHI) should be entered into the ECM Privacy Management Software. If there is an issue that arises when using ECM that prevents the release of PHI, the Department needs to alert the Privacy Officer for assistance and corrective action.

The Privacy Officer for MedSchool Associates South is:

Tammy Boring CPC

Director of Billing Compliance and Privacy Officer

2040 West Charleston Blvd. Suite #202-A

Las Vegas, NV 89102

(702) 671-6447

(702) 671-2266 fax

tboring@unr.edu email

The Privacy Officer will meet face to face with the patient if necessary to address any verbal questions as soon as possible. If there are issues that arise that need more information, research, etc then the Privacy Officer will respond to all patient questions within 30 days of the written request. The department staff will be responsible for providing the patient with the appropriate form. If there is any delay, the Privacy Officer will communicate to the patient and explain the problem and give a reasonable estimate for resolution of the patient concern. The Privacy Officer will document all of this activity in the ECM Privacy Management Software.

Section 8.0-HIPAA committee

In January, 2002, a HIPAA committee was created by MedSchool Associates South. The committee membership is composed of all Department Administrators, Director of IT, Director of Human Resources, Chief Business Officer, Director of Billing, Vice Dean and includes various members of the organization as issues arise. The committee is chaired by the Director of Billing Compliance/Privacy Officer. The mission of the committee is to develop policies and procedures related to HIPAA implementation and will provide specific Department input as the policies are created and updated. The HIPAA committee will act as the advisory body for all HIPAA related issues. The committee will become part of the complaint process if privacy issues arise that are not resolved by the Privacy Officer.

The committee has developed this policy manual as a tool to assist in the creation, training and certification of all HIPAA related policies and procedures.

Section 9.0-Sending Protected Health Information to Another Entity

This organization often finds it necessary to send a patient's protected health information to another entity for a variety of reasons. These entities fall into two categories: "known" organizations and "unknown" organizations. Before sending ANY information to either of these groups, you must follow these steps, and you may need approval from the Privacy Officer. You CANNOT disclose any information about the patient before completing these steps; unauthorized disclosures are subject to discipline, including possible termination.

"Known" Entities (Business Associates)

Sending protected health information to "known" entities generally does not require prior approval from the Privacy Officer. If, for example, the doctor has referred a patient to a specialist found on the "Known Entities" list, the specialist may need some information found in the patient's medical record.

You must first determine what information is being sent to the other entity. Most likely, the type of information disclosed fits within the "standard routine" disclosures as described on the "Known Entities" list. Verify that the information you will send falls under the minimum necessary rule and determine if you have the appropriate authority to release the information. Also, verify that you do not need an authorization for this entity; if you do, have the patient complete it prior to releasing the information. If the information does fall within the description, you may send the information to the other entity, but ONLY to the address or fax number listed on the "Known Entities" list. Sending the information to any other address or fax number requires approval from the Privacy Officer. Enter the disclosure into ECM privacy management software program. You may then send the information. Failure to enter the information into the software program will result in disciplinary action.

If the information you will send falls outside the category listed on the "known entities" list, you must review whether the information exceeds the "minimum necessary" for the other entity. You are limited to sending only the "minimum necessary" information to the other entity without the proper authorization from the patient. Similarly, if the information is not used for treatment, payment, or health care operations purposes, you MUST have the proper authorization from the patient(s) PRIOR to sending any information. Look in ECM under the Patient's name and determine that the necessary release form has been signed prior to sending this information. Please enter the appropriate ECM computer entry to document the disclosure. Failure to enter the information into the software program will result in disciplinary action.

It may be necessary to send protected health information to an organization that is not listed on the "Known Entities" list. BEFORE sending any information to the entity, you must first verify the correct address or fax number for this organization (depending on how you will send the information). After verification, you must then determine if the information is to be used for treatment, payment, or health care operations. If so, enter the disclosure in to ECM, the software will indicate to you the address on file for the entity, and then you may send the information to the other entity. Failure to enter the information into the software program will result in disciplinary action.

If the information is to be used for something other than treatment, payment, or health care operations, you **MUST** have prior authorization from the patient(s) on file **BEFORE** you may send any information. Look up the patient in ECM and check for the appropriate authorization form for this type of disclosure. If so, enter the disclosure into ECM, and you may then send the information. If there is no authorization from the patient(s) on file with the organization, you must obtain authorization using the proper authorization form. If there is nothing on file, you must obtain authorization from the patient using the MedSchool Associates South authorization form. Do not release any PHI to an “unknown” Entity without the appropriate signed authorization. Again, please document the disclosure into ECM privacy software. Failure to enter the information into the software program will result in disciplinary action.

Section 10.0-Requests for Protected Health Information

A request for patient's protected health information from another covered entity may be received by telephone, fax, mail, or in person. When such a request is received, you must follow these steps before revealing ANY protected health information. No matter how insistent the requestor, you CANNOT disclose any information about the patient before completing these steps. Unauthorized disclosures are subject to discipline procedures termination of employment.

Telephone: If the request was made using the telephone, you should inform the requestor to send you a fax on their official letterhead stating their request. You must determine if the requestor is a "known" requestor or a "known" Business Associate as recorded in the HIPAA-safe software. Oral requests from unknown individuals over the telephone are not allowed and will not be fulfilled. If the individual making the request does not wish to send a written request (either by mail or by fax), transfer them to the Privacy Officer, who will explain why oral requests are not accepted by MedSchool Associates South.

For "known" requestors and "known" Business Associates, enter the request into the ECM privacy management system. Be sure the correct date, time, name, and other information (e.g. business name, telephone, etc.) of the individual requesting the information, the patient's name, what information has been requested, and for what purpose. Be as specific as possible in describing the information requested and its purpose. If the information requested exceeds what information is the "minimum necessary" for that entity, you must first discuss the request with the Privacy Officer prior to sending the requested information.

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

Once you have verified the identity of the requestor, received the proper authorization from the patient, and entered the request into ECM, you may then send the requested information, but ONLY to the "usual" address or fax number, as listed on the "Known Entities List". Any address or fax number not contained on the "Known Entities List" requires approval from the Privacy Officer before you send ANY information.

Fax or mail: If the request was submitted via the facsimile machine or via U.S. mail, first determine the origin of the fax or letter. The document should have an official seal, logo, or other identifying mark that clearly establishes the individual or entity requesting the information. It should also include the business name, address, telephone number, and name and title of the individual making the request. The fax or letter must state clearly what information is requested, and for what purpose(s) the individual or entity will use the information. If any of these items are not on the document, or it does not give adequate details, contact the requestor to get more details about the information requested and/or the intended use of that information. Remember, it is always our policy

to deny access to the PHI until proper identification and purpose is determined. For information requested related to a legal proceeding, the fax or letter must be accompanied by a copy of an official judicial subpoena or other court document as requested by state law.

Once you have concluded the fax or letter is a legitimate request for information from another entity or individual, you must then ascertain whether the information is to be used for treatment, payment, or health care operations purposes. Any purpose outside these three areas requires an authorization from the patient before sending any information. You will then contact the patient and ask for proper authorization, or refuse the request due to a lack of proper authorization.

After you have verified the requestor's identity and received proper authorization (if necessary), enter the request into ECM. Then, if the recipient of the information is listed on the "Known Entities or Known Business Associates List" chart, you may send the information to the requestor through the listed address or fax number. If the entity is not "known" or has requested the information be sent to an address or fax number not on the list of "Known Entities", contact the Privacy Officer for his or her approval. Once you have the Privacy Officer's approval, you may send the requested information.

In person: If an individual comes in to the office and makes an in-person request for a patient's protected health information, you must verify the identity of the individual. This can be accomplished by asking for their driver's license, employment ID badge, or other picture identification. Make a copy of the identification, and then have the requestor fill out and sign the Authorization form. Then, take the completed form, the copy of the picture identification, and enter then request into ECM.

If the requestor is a public official, you must verify the identity of the individual making the request by examining an official letter from the agency or department where the individual is employed (or represents), a government identification badge, or similar proof of official status. The individual must also present to you written evidence of the agency's legal authority to obtain the information.

If the requestor is an attorney and the information is to be used in a legal proceeding, you must ask for and copy an official judicial subpoena or other official court document supporting the attorney's legal authority to request the patient's information.

Upon verification of the individual's identity and completion of the Authorization form, you must contact the Privacy Officer to approve the request. After approval and entering the request into ECM, you may then disclose the information to the requestor.

Section 11.0-Denial of Disclosure Policy of PHI

MedSchool Associates South has a policy for denial of disclosure of patient PHI in response to a request that does not fulfill the required elements for disclosure. A letter will be sent by the Privacy Officer that will explain the reasons for the denial. It will then be up to the requestor to fulfill the missing elements prior to release of the PHI. The Privacy Officer will log into the ECM program the date and reasons for the non-disclosure. This notation will become part of the disclosure log of the patient record. This log will be kept on the ECM program in case of a request by the patient for a disclosure accounting.

Section 12.0-Retention and Security of Records

Records that are considered part of the patient's treatment records (often referred to as a chart) must be retained in accordance with state law. Such original records should not be destroyed for any reason. It is the policy of MedSchool Associates South to keep all original medical records indefinitely.

We also have records pertaining to our business operations that may contain limited health information. These records must be retained for a period of at least seven years. When not in use, health information records in paper form should be kept in a locked file drawer, office or storage area. The storage area shall remain locked or access restricted at all times. Employee without proper authorization should not access these areas.

Computer systems and electronic storage of data shall be maintained in a secure facility, and reasonably appropriate security measures shall be taken to protect the security of data during storage and electronic transmission of the data. Employees without proper authorization should not access password protected data. Records in use should not be left unattended in areas where unauthorized individuals or members of the public could gain access.

Our office has implemented a system that stores protected information in a manner that reasonably keeps it away from unauthorized personnel. We use passwords on our computers and screen savers that will blank the screen or remove from view of protected information when we are not present at the computer or within a specific period of time. We keep paper records closed so that protected information is not easily viewable by others in our offices. Reports, papers with protected information and other documents are to be reasonably kept in a fashion that does not easily allow viewing by others. All non original documents that contain PHI that is no longer used will be shredded and disposed of appropriately. We retain all PHI in the medical record indefinitely. We may send old medical record information that is older than 1 year into an offsite storage facility but will still be able to be retrieve it if necessary for a patient's clinical care within a reasonable amount of time.

Section 13.0-Intake Process

Sign-in Sheet and Reception Area

Communications with patients or prospective patients in public reception or waiting areas should be kept to a minimum. Sensitive medical conditions should not be discussed in public waiting areas or reception areas. Patient sign-in sheets should clearly state that the patient does not need to disclose information on the sign-in sheet that pertains to their health condition, unless such information will be removed before another patient has access to the sign-in sheet. Reception area employees should ensure that patients do not congregate at the reception area window or near billing cubicles where patient health information may be discussed.

We have implemented a revised sign-in sheet that does not contain, or compromise, our patient's private information. Our sign-in sheet uses only the patient name and time of appointment and does not include information related to the diagnosis, financial or other protected information.

Section 14.0-Discipline of Employees

We will maintain a policy that when and if an employee violates these policies or applicable rules we promulgate in our office to supplement these policies, the employee will be disciplined by receiving notice of the infraction and/or violation. We will then take the action necessary to correct the problem with the employee, which may include termination of employment. We will document any action taken in the employee's personnel file in Human Resources. We believe that compliance with federal privacy regulations is important to our office and to our patients and we will take appropriate disciplinary action when an employee fails to abide by the regulations and these policies.

Section 15.0-Disclosure of Protected Health Information

Unless provided for in these policies or by applicable Federal law, we will not disclose PHI without the authorization. We will notify each patient of their Privacy Rights with our Notice of Privacy Practices and attempt to receive acknowledgment of these rights from the patient before we use or disclose his or her PHI for Treatment, Payment or Operations purposes as described below. Our policy is to disclose only the minimum necessary information for payment and operations reasons when such use or disclosure is required. We may rely on the representations of our Business Associates, as described below, when determining what information is required when disclosing for purposes of payment or operations. We need not obtain authorization from the patient to use or disclose for treatment, payment or operations reasons, as described below. However, we will ensure that the patient has received a Notice of Privacy Practices and Rights as well as the opportunity to acknowledge receipt of the Notice.

In the event we need to receive authorization from a patient for use or disclosure not provided for pursuant to these policies, we will do so by providing the patient with our authorization form. We will not disclose information that is not allowed to be disclosed under these policies or applicable state or federal law without the patient's authorization. An authorization must be in writing and must set forth specific circumstances for which we may use or disclose PHI. A patient may revoke their authorization in writing at any time. When we have received notice of the revocation, we will no longer disclose following receipt of the revocation.

We cannot refuse to treat a patient for refusing to sign an authorization except in situations where treatment is for research purposes, or in situations in which the treatment is solely for the purpose of disclosure to a third party. For example, if an employer agrees to pay for an employee to obtain a physical to demonstrate fitness to return to work, we may require authorization to release the record to the employer before we

provide the physical. Anything disclosed prior to the revocation was properly authorized by the patient.

A. Oral Agreement

In certain circumstances, we may not be able to obtain authorization from the patient as described above. In these rare circumstances, we may rely on the patient's oral agreement for disclosure of PHI. Sometimes, in emergency circumstances, a patient may not be able to give authorization or is unavailable. In these circumstances, we will use our best judgment before acting on behalf of the patient.

B. Access to Records

We may need to determine the identity of a patient to verify the patient. The patient has a right to review their health care records in a designated record set with a designated employee, which is essentially the patient's chart. The patient is also entitled to obtain a copy of these records for a fee of .60 cents per page and the actual cost of postage.

We require the patient to make this request in writing. Forms have been prepared for this purpose. Normally we will allow the inspection within 15 days and will make copies available within 30 days.

There are limitations on the patient's right to access and copy health records. For example, a patient is not entitled to review a copy of psychotherapy notes (do we want Genetics added?) as described in HIPAA. A patient is also not entitled to review information compiled for legal proceedings. There may be other situations in which a medical provider may deem it necessary to suspend a patient's right to access medical records based on concerns for the well being of the patient or another individual. We may also deny access to information obtained from others under an agreement of confidentiality. In these rare circumstances, we may obtain appropriate identification such as a drivers license or similar picture ID.

Section 16.0- Types of Uses and Disclosures Without Authorization

A. Treatment

We have the right to use and disclose PHI for treatment purposes without authorization. For example, information may be used and exchanged by physicians, nurses, nurse practitioners, or other medical professionals, staff, trainees, and volunteers in our office in order to treat the patient. While the minimum necessary rule does not apply to such disclosures, medical providers should be careful about disclosures of protected health information, particularly sensitive health information, such as communicable diseases, in areas in which other patients may overhear the information. In situations where sensitive information needs to be discussed with the patient, efforts should be made to ensure that those communications occur in private. We may communicate with a patient regarding appointment reminders and follow-up care.

B. Payment

We may communicate PHI to an insurance company and others without authorization only as necessary to obtain payment on a claim. This information may identify the patient, as well as the diagnosis, procedures and supplies used as necessary to obtain payment. If the patient is not seeking reimbursement or payment for a particular treatment, we should not disclose the patient's entire medical record to the insurance company.

These disclosures are limited to the billing/payment function only. For example, we should not disclose a patient's health information to an insurance company in order to determine the insurability of a patient, unless the patient has specifically authorized the disclosure of the patient's medical records for that purpose.

C. Healthcare Operations

We may use PHI for healthcare operations without authorization. This means, for example, that members of the medical staff, trainees, medical students, a risk assessment or quality improvement team or similar internal personnel may use PHI to access the care and outcomes of a patient's care in an effort to improve the quality of the healthcare or for educational purposes. For example, an internal review team may review PHI to determine the appropriateness of care.

In addition, from time to time other personnel employed by use or by the University System may need access to PHI to meet their job responsibilities. For example, accountants and auditors may have to review PHI if necessary to properly perform an audit. As another example, our attorneys may be required to review PHI in order to give us proper legal advice.

D. Marketing and Fundraising

From time to time we may contact patients, without authorization from the patient, about treatment alternatives or other health related benefits and services that may be of interest to the patient. Patients may also be contacted regarding fund raising efforts. All such contacts must be pre-approved and may not be for personal purposes.

Section 17.0- Other Uses and Disclosures Not Requiring Authorization

A. Business Associates

We have contracts with outside vendors to perform certain services on our behalf. If these services involve the disclosure of PHI, these vendors are known as "business associates," and we are required to have a specific written contract with these vendors to ensure that they comply with HIPAA requirements. In these circumstances, authorization is not required to disclose PHI to the business associate. An example of business

associates might include outside laboratory or radiology services, software companies assisting in the handling of PHI, and companies that assist us in billing.

If a business associate violates privacy rules, we have a right to demand that the business associate correct the problem. We may also choose to terminate the contract with the business associate.

B. Notifications to Friends and Family

We may be asked for information about a patient by a friend or family member involved in the patient's care, or assisting the patient in paying for services. During intake, the patient should indicate whether there are family members, friends, or others with whom we can communicate regarding the patient's condition. In emergencies, however, we may disclose limited information without authorization about the patient's location and general condition to family members, friends or others that we reasonably believe may be involved in the patient's care. In some situations, such as suspected child abuse or domestic violence, we may choose not to disclose any information, including the whereabouts of the patient, to a friend or family member.

C. Public Health Disclosures or Threats to Health and Safety

We are allowed to disclose PHI without authorization in numerous circumstances authorized by law, or as necessary to avert a serious threat to health or safety. A number of examples that allowed under HIPAA, and any limitations, are discussed below.

a. Communicable Disease

State law allows us to disclose PHI to identify exposure to, and prevent the spread of, communicable disease, but it does not allow us to identify the individual(s) involved. We may, however, be required to disclose this information to appropriate health authorities.

b. Child Abuse

We are required to report situations in which we believe that child abuse or neglect has occurred to the appropriate governmental authorities. We will report this information without seeking authorization.

c. Domestic Violence

We may report information pertaining to domestic violence to appropriate governmental authorities without authorization. We will first seek to notify suspected victims of domestic violence of our intention to disclose this information to the appropriate governmental authorities.

d. FDA Regulated Products

We may disclose PHI pertaining to the quality, safety or effectiveness of FDA regulated products or activity to the FDA without authorization.

e. Worker's Compensation

We may disclose PHI without authorization to an employer, or allow an employer to conduct medical surveillance of the workplace, solely in order to evaluate whether an employee has work related illness or injury.

f. Health Oversight Agencies

We may disclose PHI without authorization as necessary for public health oversight authorities so they can monitor, investigate, discipline, or license those who work in the health care system or for government benefit programs.

g. Public Reports

We may report births and deaths without authorization.

D. Law Enforcement

We may disclose PHI to law enforcement without authorization in the following circumstances:

1. Identification and Location

We may disclose PHI solely for identification and location purposes.

2. Victims of Crime

We may disclose PHI regarding suspected victims of crime. Before releasing this information, we will first attempt to obtain an agreement from the suspected victim to release the information.

3. Deceased Individuals

We may disclose PHI about a deceased individual if we have a reasonable suspicion that the death resulted from criminal conduct.

a. Crime in connection with our operations

We may disclose PHI that we believe in good faith establishes that a crime may have been committed on our premises. We may also disclose PHI

regarding a crime occurring off our premises during our providing of emergency healthcare.

b. Armed Services

For patients who are members of the armed services, we may disclose certain PHI requested by the armed services.

c. National Security

We may disclose PHI as requested by national security and intelligence operations, or for protective services for certain governmental officials

d. Inmates

If a patient is an inmate, we may disclose PHI to correctional officials for health and safety purposes.

E. Subpoenas and Court Orders

We may disclose PHI without authorization as required by a court order or an administrative order. We will also disclose PHI without authorization in response to a valid summons or subpoena. If an employee receives a subpoena or court order, it should be forwarded immediately to administration.

If the subpoena is for a civil court action, we will typically contact the patient at the patient's last known address, or the patient's attorney, if known, to inform the patient of the subpoena, to provide the patient with a copy, and to inform the patient of our intent to provide all responsive documents on or prior to the date identified in the subpoena. This is not required if the patient is a party to the lawsuit. Alternatively, we may ask the requesting party for assurance that reasonable efforts have been made to inform the patient of the subpoena.

F. Information Regarding Decedents

We may disclose information without authorization regarding a deceased person to:

- a. Coroners and medical examiners to identify cause of death or other duties;
- b. Funeral directors for their required duties; and
- c. Procurement organizations for the purposes of organ and tissue donation.

G. Research

We may disclose protected health information for research purposes without authorization for the purpose of designing a study. In this situation, no PHI may be removed from our facility. We may also disclose PHI for research without authorization

where disclosure concerns decedents, or an institutional review board or privacy board approves the disclosures, and the board has determined that obtaining authorization is not feasible. The Board should also determine that protocols are in place to ensure the privacy of health information. Our institutional review board or privacy board must approve all research involving human subjects that is undertaken by researchers employed by us.

H. Directory Information

We may disclose without authorization information regarding a patient's name and location for directory purposes to those persons who ask for a patient by name. We may also disclose information regarding religious affiliation and location to clergy. Patients have the right not to include their name in the directory.

I. Regulatory and Audit Disclosures

We may be required to provide information to authorized enforcement and regulatory agencies from time to time. Such information will be provided subject to the law and pursuant to the requests of the authorized agency. We may disclose information for audit purposes and for complaint management both internally as part of our internal operations and, upon request, to the United States Department of Health and Human Services.

Section 18.0-Minimum Necessary Information Only

We will make reasonable efforts to disclose only the minimum necessary information to the receiving party pursuant to applicable state and federal requirements. We are not required to apply the minimum necessary rule to disclosures made for Treatment, as described above, for disclosures to the patient, disclosures to the Department of Health and Human Services for compliance reviews or complaint investigations, disclosures required by law or use or disclosures required to comply with the federal Health Insurance Portability and Accountability Act provisions. Within our office, we will also follow the minimum necessary rule in our use of a patient's PHI.

Section 19.0- Amendment to Medical Record

Pursuant to the Privacy Regulations, patients may request that we amend their records. We will make a decision regarding the amendment based on the documentation provided by the patient. Amendment does not require us to delete information from the record. We may allow the patient to add information to the record or, if we believe it is appropriate, we may change the record based on the request of the patient. If we did not create the information (unless the entity that did is not available to allow the amendment) we believe the information is accurate and complete or if we do not have the information, we may deny the patient's request to amend. We will follow the Federal Privacy regulations when determining if it is appropriate to allow or deny a patient's amendment request.

As noted above, we will not physically delete or alter information already contained in the patient's record. We will, however, allow information to be added, when appropriate under the rules and within our professional judgment, as noted above. In the event we agree to make an amendment, we will notify our Business Associates that may have the patient's PHI, of the amendment, so they may adjust their records as well. If we sent out information that was erroneous or incorrect in regard to the PHI, we will reasonably notify any entity that may have received the erroneous information. In the event we deny a patient's request for amendment, in any future disclosure of PHI, we will note in the record that we denied a request for amendment.

Section 20.0-Disclosure Accounting

We will provide accountings of disclosures as required by law. Under the law, we are required to keep track of certain disclosures we make of a patient's PHI. The rules do not require us to track disclosures for purposes of Treatment, Payment or Operations, as described above. We do not need to track disclosures related to national security, correctional institutions regarding inmates or when provided an authorization by the patient or his/her personal representative. We may suspend accounting if required to do so or allowed for under the Privacy rules or authorized regulatory agency. We will use the ECM software program to track the disclosures that we make. We may charge for an accounting that is more frequent than every twelve (12) months. The patient will be notified of the fees for such an accounting.

We are also required to provide an accounting of disclosures made by our Business Associates. Upon request by the Patient, we will notify our Business Associates of the requirement that they provide an accounting of any permissible disclosures they have made.

Section 21.0-Request to Restrict Disclosure

Patients may request that we restrict disclosures that we make of their PHI. We have no obligation to comply with these requests, but if we do, we will comply with the restriction. Any request must be made in writing. If we do agree to the request, we may still disclose the information if it is required in an emergency situation. If we agree to a restriction, we will promptly notify any affected Business Associate. We may terminate the restriction by giving written notice to the patient of our decision to do so. We will use ECM to track any restrictions.

Section 22.0-Alternative Communications

Patients have the right to ask us to use alternative ways or locations when communicating PHI to them. A patient has a right to request that we limit the means of communication with that patient. For example, a patient may request that we contact the patient by mail only, except in the case of an emergency. Our offices will accommodate such requests when made in writing and when such request is reasonable. Our offices will notify the patient of our decision to accommodate any of this type of request. We

will notify the patient of what will be required in order for us to meet their request. In some cases, there may be a fee associated with meeting a patient in an alternate location. The fee will be reasonable and we will only accommodate when such request and location are reasonable.

Section 23.0-Documentation of Privacy Activities

We will use ECM to document our privacy practices and actions. Our internal policy is to use ECM to track information and to assist in our management of privacy related activities. It shall be the duty of the Privacy Officer to ensure employees are following these policies and using ECM appropriately to track our privacy related activities. Failure to document information into ECM will result in disciplinary action.

Section 24.0-Initial Privacy Assessment

We have done an initial privacy assessment using ECM and will take steps to ensure that our offices meet the Federal regulations, including those that may not be included in ECM, in becoming Privacy compliant. We have conducted this assessment in a reasonable period of time to ensure we are compliant in accordance with the Privacy regulations. In the event our state has laws that are more stringent than the Federal requirements, we have incorporated policies that supplement these policies to ensure we meet state requirements as well.

Section 25.0-Complaint Manager

We will manage complaints made by patients with respect to Privacy. Complaints will be directed to the Privacy Officer who shall attempt to resolve the complaint after determining the type, validity and circumstances contained in the complaint. We would prefer the complaint be in writing and addressed to the Privacy Officer. We will accept Privacy complaints verbally but will request the patient to document for tracking purposes. In the event the complaint is made to DHHS, the designated complaint manager a.k.a. the (Privacy officer) shall work with the Department to resolve the issues. Should the resolution require modification of these policies or changes in operation and/or personnel, appropriate action will be taken. A patient that requests the address of DHHS shall be immediately provided with that information. This office shall not retaliate against any patient or person making a complaint pursuant to the Privacy or any other governing regulations.

Section 26.0-Appeals Process

If a patient does not think that his/her issue has been resolved by the Privacy Officer, the patient may then request an appeal in writing and submit it to the Privacy Officer. The Privacy Officer will bring the issue to the HIPAA committee members for a resolution. The committee will review the facts and give a recommendation of their decision in writing to the patient. If the issue is still unresolved, the patient will be directed to pursue the final course of action with the Vice Dean's office of the School of

Medicine. The issue may or may not be addressed by the Vice Dean. The patient will then have a written response from the Vice Dean's office regarding the decision. This is the conclusion of MedSchool Associates South internal privacy policies and procedures for HIPAA. These policies are subject to review at least annually.

HIPAA Employee Verification of Understanding of Policies Regarding Patient Confidentiality and Privacy

Acknowledgement

I have received a copy of the Privacy Policies of MedSchool Associates South, Inc. Including the Confidentiality of Clinical Information and the MedSchool Associates South Inc. Policy on the Disciplinary Process for Breach of the Patient Confidentiality. I have read the Policies and understand their contents. I have been trained on the policies and procedures in this manual and agree to follow these privacy policies and procedures. I agree to keep all MedSchool Associates patient information as outlined in the Policies strictly confidential. I understand that breach of patient confidentiality as defined in the Policies will result in disciplinary actions, up to and including termination of employment.

Employee Name (print) _____

Employee Signature _____

Date _____