ADMINISTRATIVE SAFETY PROCEDURES AND POLICIES

SCNM Medical Center Procedure:

Purpose of Procedure: To prevent the spread of germs

Procedure Title: Cleaning Exam Room	**Procedure Number: 0015**
Department/Staff: SCNM Students/Physicians/MA	
Effective Date of Procedure: **Procedure Updates:** 10/23/14	
Procedure Approved by: Medical Center Steering Committee	**Signatures:**
Procedure Implemented by: Medical Center Safety Committee	**Signatures:**

Procedure:

Any room used for patient care will be wiped down with antiseptic wash (ie hydrogen peroxide wipes or wash, Cavicide wipes or wash) per manufacturer instructions after each patient.

This includes:

- Exam Table
- Chairs
- Pillows
- Counter top
- Mayo stand
- Any surface where patient came in contact with

SCNM Medical Center Procedure:

Purpose of Procedure: To ensure disposal of non-contaminated broken glass is handled safely and promptly.

Procedure Title: Disposal of Non-contaminated Broken Glass	**Procedure Number: 0055**
Department/Staff: Medical Center Employees	
Effective Date of Procedure: 1/12/11 **Procedure Updates:** 4/27/11, 2/11/15	
Procedure Approved by: Executive Vice President of Academic and Clinical Affairs	**Signatures:**
Procedure Implemented by: Director of Clinical Operations	**Signatures:**

Procedure:

1. Clear area where the broken glass has occurred.

2. Contact Patient Services and put out yellow caution sign in the area.

3. Patient Services to contact Facilities regarding broken glass.

4. Once Facilities personnel have completed removing the broken glass and has deemed area safe, area will be available for patient care.

Medical Center Procedures:

Purpose of Procedure: To ensure that expired drugs and medical materials are identified and disposed of in a timely manner.

Procedure Title: Expired Products	**Procedure Number:**
Department/Staff: Medical Center	
Effective Date of Procedure: **Procedure Updates:**	
Procedure Approved by:	**Signatures:**
Procedure Implemented by:	**Signatures:**

Procedure:

1. General Storage, exam rooms and prep areas will be checked for expired products every 30 days by designated staff.

2. Expired products will be pulled from the shelves, replenished and disposed of properly.

3. If vendor does not have an exchange program for expired products.

4. Disposal according to the directions on bottle.

5. If the answer to number 3 and 4 is no, refer to the following instructions:
    a. Liquids-empty into a sealable bag with coffee or cat litter to absorb liquid. If not biohazard material, dispose of in trash.
    b. Needles and sharps: empty in sharps container.
    c. Non-biohazard material: empty in trash.
    d. Biohazard material: empty in biohazard safe container.

SCNM Medical Center Procedure:

Purpose of Procedure: Provide instructions for safely exiting the Medical Center in case of fire, smoke, explosion or other disaster.

Procedure Title: Fire Evacuation	**Procedure Number: 0016**
Department/Staff: Medical Center Staff, Physicians and Students	
Effective Date of Procedure: **Procedure Updates:** 3/28/11, 9/26/13, 7/23/15	
Procedure Approved by: Executive Vice President	**Signatures:**
Procedure Implemented by:	**Signatures:**

Procedure:

When a fire is discovered:

1. **RACE – word to remember**
    a. **R**ESCUE
    b. **A**LARM (911)
    c. **C**ONTAIN FIRE
    d. **E**XTINGUISH FIRE
2. When a fire is discovered, notify patient services staff to page a CODE RED and location of Code Red. Patient Services will then page a Code Red and location of Code Red.
3. Patient Services staff will call 911 or push fire alarm button for two seconds on security alarm panel when notified.
4. Patient Services will notify Facilities of fire and location.
5. Evacuation location for all individuals in the 2164 building will be just outside the northwest end of the parking garage.
6. Check-in person is to take the daily master schedule and the list of students on rotation with them when exiting the building for safety.
7. Following departments in the Medical Center will be responsible to clear the following areas and report to the are just outside the northwest end of the parking garage East of the Medical Center Building:
    - Patient Services –
        - Reception waiting area, Public restrooms in lobby by elevator and master list. Exit through main clinic doors
        - Exam rooms 1-10; hall restroom; Classrooms A, B. Exit through west stairwell door.
        - Exam rooms 11-15; Classrooms E, F. Exit through west stairwell door.
    - Lab – Exam rooms 16-19; Administrative Office; Staff Physician Office; IV Room; Classrooms C & D; Restroom outside of lab. Lab personnel are to leave building near Classroom B

- Medical Assistants – Exam rooms 20-27; hydro-suite (steam room, saunas, locker rooms) and old Medicinary area. They will leave through the east stairwell door.
- Physicians on student rotations are responsible for evacuating their classrooms.

8. As rooms are cleared, a sticker to designate the room has been checked and cleared will be placed on the door. Stickers will be located in each department.
9. Individuals checking areas are to report to Facilities Manager or staff as directed when their area is cleared.
10. When Fire Department has given the all clear to return inside the building, Facilities will notify everyone if able to function in building.
11. Patient Service Representatives will take names and phone numbers of the patients to reschedule appointment.
12. Once determination is made as to time for repairs, patients having appointments during time of repair will be contacted and appointments will be rescheduled.

Fire extinguisher use includes:

1. **PASS**
    a. **P**ULL THE PIN ON THE EXTINGUISHER
    b. **A**IM
    c. **S**QUEEZE THE HANDLE
    d. **S**WEEP

SCNM Medical Center Procedure:

Purpose of Procedure: To document medical emergency procedures.

Procedure Title: Medical Emergency	**Procedure Number: 0011**
Department/Staff: Medical Center Employees	
Effective Date of Procedure: **Procedure Updates:** 3/28/11, 2/4/15	
Procedure Approved by: Executive Vice President	**Signatures:**
Procedure Implemented by:	**Signatures:**

Procedure:

1. When medical emergency is identified, notify Patient Services with location of emergency.
2. Patient Services will page a CODE PURPLE and identify location of emergency.
3. All available clinic physicians MUST report to the room immediately.
4. Attending physician will take the lead, but may defer to another physician with more experience/expertise.
5. Patient will be medically stabilized within the capabilities of the Medical Center.
6. Patient's status will be assessed by the lead physician and a decision made as to whether to transport to an emergency facility.
7. If transport is deemed necessary, 911 will be called by patient services or alert via alarm system by pressing medical button for two seconds.
8. Lead physician or their designate will contact the hospital to which the patient will be transported and let them know of the patient's status, probable diagnosis and relevant treatments. This interaction will be charted.
9. If the patient is stabilized, and transport is not deemed necessary, the patient will be observed at the Medical Center for a period of time afterward to ensure they will not have a recurrence of the event.
10. All treatments rendered at the Medical Center will be charted.
11. Patient will be contacted by attending physician within 24 hours of discharge from the Medical Center in order to assess their continued stability, and patient contact will be documented in the chart.

SCNM Medical Center Procedure:

Purpose of Procedure: To outline procedures that assures adequate availability and training regarding Personal Protective Equipment (PPE).

Procedure Title: Personal Protective Equipment Procedure	**Procedure Number: 0041**
Department/Staff: Medical Center Employees	
Effective Date of Procedure: 9/10/10 **Procedure Updates:** 10/23/14	
Procedure Approved by: Medical Center Steering Committee	**Signatures:**
Procedure Implemented by: Medical Center Safety Committee	**Signatures:**

DEFINITIONS:

PPE includes:

- Protective shields and barriers (i.e., gloves, face masks, goggles, face shield, etc.)
- Protective clothing (i.e., gowns, booties, etc.)
- Design:
    - All PPE shall be of safe design and construction for the work to be performed

PROCEDURE:

PPE will be provided, used, and maintained in a sanitary and reliable condition. Protective equipment will always be used when hazards are capable of causing injury or impairment in the function of any part of the body (eyes, face, head, torso, and extremities) through absorption, inhalation, injection, or ingestion.

Responsibilities:

1. Employees: If employees require special PPE other than what is normally provided, a request will be made to immediate supervisor. Supervisors shall assess the workplace to determine if hazards are present, or are likely to be present and select, fit, and test as needed for each affected employee.

2. All PPE will be removed and properly disposed of when leaving patient room or when grossly soiled.

3. Defective or damaged PPE shall not be used.

Training:

1. The Medical Center Management shall provide annual training to each employee who is required by this section to use PPE. Each such employee shall be trained to know at least the following:

a. When PPE is necessary
b. What PPE is necessary
c. How and when to properly don, doff, adjust, and wear PPE
d. The limitations of the PPE
e. The proper care, maintenance, useful life, and disposal of the PPE

2. Each employee shall demonstrate an understanding of the training and the ability to use PPE properly, before being allowed to perform work requiring the use of the PPE.

3. When the supervisor has reason to believe that any employee, who has already been trained, does not have the understanding and skill required, the employer shall retrain each such employee. Circumstances where retraining is required include, but are not limited to, situations where:

    a. Changes in the workplace render previous training obsolete
    b. Changes in the types of PPE to be used render previous training obsolete
    c. Inadequacies in an affected employee's knowledge or use of assigned PPE indicate that the employee has not retained the requisite understanding or skill
    d. Employee may be disciplined up to and including termination for lack of ability or refusal to adhere to the PPE procedure.

SCNM Medical Center Procedure:

Purpose of Procedure: To ensure that all medical equipment is maintained to function properly and reliably

Procedure Title: Preventative Maintenance of Medical Equipment	**Procedure Number: 0044**
Department/Staff: Medical Center Employees	
Effective Date of Procedure: 9/10/10 **Procedure Updates:** 5/25/11, 2/15/15	
Procedure Approved by: Executive Vice President of Academic and Clinical Affairs	**Signatures:**
Procedure Implemented by: Manager of Medical Center	**Signatures:**

.

Procedure:

1. SCNM contracts with a company qualified to provide preventative maintenance and repairs on medical equipment. Contractor is responsible for ensuring inspections and maintenance of medical equipment is performed by qualified person(s).

2. On an annual basis, contractor comes on site to provide preventative maintenance, to include calibration, on all medical equipment.

3. All new equipment is calibrated prior to use by a qualified technician.

4. Should a piece of medical equipment malfunction or operate with questionable accuracy, staff will remove the piece of equipment from use/circulation and contact contractor for evaluation and repair.

5. All documents regarding maintenance are kept in the office of the Manager of Medical Center.

SCNM Medical Center Procedure:

Purpose of Procedure: To protect the confidentiality of patient information

Procedure Title: Shredding Paperwork	**Procedure Number: 0030**
Department/Staff: Medical Center Employees	
Effective Date of Procedure: **Procedure Updates:** 8/10/11, 2/11/2015	
Procedure Approved by: Executive Vice President	**Signatures:**
Procedure Implemented by:	**Signatures:**

Procedure:

1. All paperwork containing names, personal medical records, reports, billing information, patient demographics, and other medical center forms, and private information will be shredded.

2. Any possible paperwork that contains names, personal medical records, reports, billing information, patient demographics, and other medical center forms and private information to be placed in the shredding bins.

3. Shredding company empties and shreds the paperwork in the parking lot of the facility, which occurs every two weeks.

Health Insurance Portability and Accountability Act (HIPPA)

SCNM

SOUTHWEST COLLEGE OF NATUROPATHIC MEDICINE & HEALTH SCIENCES

Medical Center

HIPPA PROCEDURES MANUAL

December 3, 2012

This document contains the procedures to be followed by all workforce members and contractors of SCNM to comply with privacy and security provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Questions concerning the contents of this document should be referred to THE DCO at 480.970-0000.

Table of Contents

Privacy Official Job Description

Actions to be taken for the privacy official job description

1. Director of Clinical Operations (DCO) has been appointed as the Southwest College of Naturopathic Medicine - Medical Center's (SCNM) "privacy official". The privacy official and the Chief Medical Officer (CMO) will be responsible for completing the job description for the privacy official.
2. The privacy official has met with the CMO in charge to review the HIPAA Privacy rule and to determine the responsibilities of the privacy official.
3. The DCO and the CMO have agreed to the following job description.

PRIVACY OFFICIAL JOB DESCRIPTION

Job Title: Privacy & Security Official

Job-Sharing: Yes-this job is performed by the DCO

Job Description:

The privacy official is responsible for implementing and maintaining the Medical Center's HIPAA Privacy and Security requirements.

Reporting structure:

The privacy & security official reports directly to the Executive Vice President of SCNM.

Job Duties:

1. Develop, implement and maintain SCNM's HIPAA Privacy and Security policies.
2. Develop, implement and maintain SCNM's HIPAA Privacy and Security procedures and forms.
3. Develop and implement SCNM's HIPAA records filing system.
4. Handle all patient privacy complaints in accordance with SCNM's complaint procedure.
5. Mitigate the effects of any unauthorized use or disclosure of Protected Health Information (PHI) or other privacy and security violations.

6. Implement appropriate safeguards for protection from intentional or unintentional unauthorized uses and disclosures of PHI.
7. Handle all patient requests for access to their PHI in accordance with SCNM's access procedure, including requests for access to psychotherapy notes as well as requests for information related to minors and requests from minors.
8. Handle all patient requests for amendment to their PHI in accordance with SCNM's amendment procedure.
9. Handle all patient requests for alternate confidential communication channels in accordance with SCNM's confidential communication channel procedures.
10. Handle obtaining individual permission from patients, or their personal representatives including oral permission and authorizations in accordance with SCNM's individual permission procedure.
11. Handle requests for special privacy protections in accordance with SCNM's special privacy protection procedures.
12. Handle the publishing and maintenance of SCNM's Notice of Privacy Practices in accordance with SCNM's procedure for notice.
13. Handle obtaining written acknowledgements of receipt of SCNM's Notice of Privacy Practices in accordance with SCNM's acknowledgement procedure.
14. Handle review and response to requests for an accounting of disclosures in accordance with SCNM's procedure for disclosure accounting.
15. Handle access requests by law enforcement, subpoenas, court orders, and public purpose entities in accordance with SCNM's procedures for this access.
16. Handle patient requests to designate a personal representative in accordance with SCNM's personal representative procedure.
17. Handle requests for access, amendment, confidential channels, obtaining acknowledgement, special privacy protections, and other requests from the patient's personal representative in accordance with the relevant procedure for these requests.
18. Handle requests for access to PHI related to deceased individuals in accordance with SCNM's procedure on deceased individuals.
19. Ensure the minimum necessary rule is applied to access, request and disclosure events within this practice, in accordance with SCNM's minimum necessary procedure.
20. Ensure regulatory currency for this practice in accordance with SCNM's regulatory currency procedure.
21. Ensure that records are retained in accordance with SCNM's records retention procedure.
22. Handle all workforce training and awareness programs in HIPAA Privacy and Security requirements in accordance with SCNM's workforce training procedure.

23. Handle all workforce sanctions where any member of SCNM's workforce intentionally or unintentionally violates any of this practices privacy or security policies.
24. Ensure all business associates are identified and have signed business associate agreements in accordance with SCNM's business associate policy.
25. Cooperate with any privacy investigation by the Department of Health and Human Services.
26. Handle any other privacy and security practice as defined in SCNM's Notice of Privacy Practices.

Implementing the HIPAA records filing system

Actions to be taken for records filing

1. The DCO has been appointed as SCNM's "privacy official". The privacy official will be responsible for developing and maintaining a HIPAA records filing system. The privacy official has met with the CMO to review the filing system procedures.

2. The privacy official has reviewed our professional liability carrier's guidance regarding HIPAA records retention and appropriate filing systems.

3. Modify our patient medical record to include a new tab for HIPAA forms related to amendment, alternate communication channels and personal representatives as well as other relevant or related forms.

4. In collaboration with the CMO, implement a separate medical record for psychotherapy notes.

5. Establish a locked, or secure files for all HIPAA records.

6. Established an alphabetical filing system with separate files for each HIPAA Privacy form we use. As request, response and tracking forms are replaced from medical records (where appropriate) ensure they are filed in the central file.

7. File all complaint forms and subsequent tracking or response in a separate file in the locked file titled "complaint forms".

8. File the business associate agreement log in the locked file in a separate file titled "business associate agreement log".

9. File the HIPAA Rule Training booklet/Acknowledgement quiz/certification statements in the Employee File.

Regulatory Currency

1. The DCO has been appointed as SCNM's "privacy official". The privacy official will be responsible for regulatory currency in this practice.

2. The policies, procedures and mandatory documents for this organization are current with state law and pre-emption requirements.

3. New updates are the primary way for this practice to learn about changes in HIPAA regulations.

4. Make relevant changes to our policies, procedures and forms as identified in the update specific to regulatory changes.

5. Train each member of the workforce who has a job function affected by the regulatory change.

6. Use the following information sources to remain current on regulatory changes and their impact:

    - Regular review of the DHHS HIPAA website

Actions to be taken for obtaining individual permission

1. The DCO has been appointed as SCNM's "privacy official". The privacy official will be responsible for obtaining written authorizations and for instructing staff who obtain verbal agreement from patients relating to the uses and disclosures of their health information.

2. The privacy official has met with the CMO to review the individual permission procedures, and has incorporated those procedures relevant to written authorization in the form for authorizing the use or disclosure of PHI.

3. The privacy official has reviewed our professional liability carrier's guidance regarding individual permission procedures and determined that this procedure comply with their guidance.

Handling requests from personal representatives

1. Determine if the request or authorization is signed by a personal representative rather than the patient.

2. Determine whether the person who has signed the request or authorization is legally entitled to serve as the patient's personal representative. InArizona, the following individuals are authorized to serve as a personal representative:

   For incompetent adults:

   - An agent pursuant to an advance directive for health care
   - A conservator of the person where the court has determined the patient lacks capacity to make health care decisions
   - A surrogate designated by the patient personally to the supervising health care provider (but only during the course of treatment or illness or during the stay in the health care institution where the surrogate designation is made or for sixty (60) days, whichever period is shorter)
   - The closest available relative or registered domestic partner where there is no agent, conservator or surrogate and their authority is not contested by anyone

   For minors:

   - Parent or legal guardian (except where the minor has the right to consent to the medical care at issue)

- The minor, but only where the minor has the right to consent to the medical care at issue

For deceased patients:

- Beneficiary or personal representative

3. Follow the established a procedure for handling requests and authorizations made on behalf of patients by their personal representatives, once such personal representative is determined as valid. Make the choice not to treat the person as a personal representative if 1) there is a reasonable belief the patient has been or may be subjected to domestic violence, abuse or neglect by such personal representative or 2) treating such person as a personal representative could endanger the patient and in the professional judgment of the CMO it is not in the best interest of the patient to treat such person as a personal representative. In this case, notify the requestor in writing as follows: “Your request is denied because the patient’s personal representative is not entitled to (type of request denied) under these circumstances." This analysis will be made with respect to each request submitted by a personal representative. Where this denial is likely to provoke a reaction, contact our professional liability carrier or attorney. Where the request is for access to PHI, the personal representative will be informed of his or her right to reconsideration of the denial.

Obtaining Written Authorization

1. Complete and maintain an accurate and up to date list of PHI that requires authorization. Currently this organization has identified the following as requiring an authorization:

    - Disclosure of medical records for a life insurance, disability insurance or health insurance underwriting of a new policy for an existing patient.
    - Note: HIPAA requires an authorization for any marketing related activities.
    - In certain cases, psychotherapy notes.

2. Ensure that all clinical research trials conducted by this organization integrate an **Authorization** into the informed consent form signed by the patient.

3. Ensure that all marketing activities to our patients have a valid authorization first. According to the HIPAA and privacy policies of this practice, we consider marketing any communication intended to induce a

purchase or use of a product or service where an arrangement exists in exchange for direct or indirect remuneration, or where this organization encourages purchase or use of a product or service directly to patients. This organization does not consider the communication of alternate forms of treatment, or the use of products and services in treatment, or a face-to-face communication made by us to the patient, or a promotional gift of nominal value given to the patient to be marketing, unless direct or indirect remuneration is received from a third party for the communication and the communication is not to a health plan enrollee concerning 1) a provider's participation in the health plan's network, 2) the extent of covered benefits, or 3) the availability of more cost-effective pharmaceuticals.

4. The privacy official will periodically evaluate any new activities, programs or related services this practice offers its patients to determine if these are marketing activities. If so, we will immediately begin to obtain a signed authorization first from each patient prior to engaging in the marketing activity on their behalf. The privacy official will seek the help of legal counsel or other expert assistance if in doubt about whether an activity of this practice constitutes marketing.

5. This organization may make remunerated communications tailored to individual patients with chronic and seriously debilitating or life-threatening conditions for the purpose of educating or advising them about treatment options or maintaining adherence to a prescribed course of treatment, without a signed patient authorization. If we do so, we will disclose in at least 14-point type the fact that the communication is remunerated, the name of the party remunerating us, and the fact the patient may opt out of future remunerated communications by calling a toll-free number. This organization will stop any further remunerated communications within 30 days of receiving an opt-out request.

6. This practice will not disclose psychotherapy notes without patient authorization (a written authorization form) except as follows:

   - **use** by the physician who created the psychotherapy notes for treatment;
   - **use** or **disclosure** by the physician for the physician's own training programs;
   - **use** or **disclosure** by the physician to defend against a legal action or other proceeding brought by the patient;
   - **use** or **disclosure** to the Secretary of DHHS in conjunction with HIPAA enforcement;
   - **use** or **disclosure** required by law;
   - **use** or **disclosure** for health oversight activities concerning the physician who created the notes;
   - **use** or **disclosure** to the coroner or medical examiner; or

- **use** or **disclosure** as necessary to comply with the physician's obligations to make Tarasoff warnings.

Moreover, to the extent these involve outpatient psychotherapy notes, this practice will further require a formal written request by the requestor, in compliance with Arizona law, except with respect to disclosures for diagnosis or treatment, for health oversight activities, or for disclosures required by law.

7. The privacy official will ensure that the appropriate authorization forms or opt out form (described in item 5) are available to the front office staff or other staff. Staff will periodically be reminded that these forms must be completed.

8. Coordinate with the front office staff to obtain a written authorization from those patients where this organization will be disclosing PHI that requires authorization. This will include appropriate modification of the "Authorization for Use of Disclosure of PHI" template on Version 2.0 or 3.0 as necessary to ensure the appropriate specificity related to the circumstances.

9. Review all completed authorizations to ensure they are valid and not defective.

10. Ensure that all authorizations provided to patients are printed in a legible font type size.

11. Ensure that a written authorization is on file prior to the disclosure of PHI for those purposes outlined in item 1 above, and for any other disclosure not excepted from the written authorization requirement in the organization's "Notice of Privacy Practices." Retain a copy of the authorization in the medical record under a separate tab and also in this organization's HIPAA Compliance file.

12. Provide the patient with a copy of the completed authorization.

13. Do not condition treatment or future care because of a patient's refusal to sign an authorization, except with respect to services that would otherwise be performed solely for the purpose of disclosure to a third party, to certain research-related treatment, and to enrollment or eligibility determinations by health plans.

14. Ensure that items 7 through 12 above are in place for the opt-out form used for tailored communications (see item 5).

15. If applicable, the privacy official will develop a process to ensure that opt out requests are handled promptly and according to item 5.

16. Only consider revocations of the original authorization when in writing; document the date when written revocation is received. The revocation does not affect actions taken prior to its receipt.

Verbal Agreement

1. Where feasible, seek a patient's verbal agreement to release or disclose PHI to a family member or friend involved in the patient's care before each such disclosure.

2. Train all clinical staff on this requirement and the importance of documentation.

3. Whenever a patient presents with a family member or friend who is not a personal representative, train the clinical staff to ask the patient if they object for this person having access to PHI for the purposes of the patient's treatment. If they object, no PHI will be disclosed.

4. If a patient wishes a family member or friend who is not a personal representative to have routine access, ask the patient to complete either an authorization or an Advance Health Care Directive form for this purpose.

5. Train front and back office staff, including the physician and providers not to discuss or disclose any information pertaining to the patient to any individual who has not been granted permission as provided in step 4, except in an emergency or where the patient has not objected to the disclosure and the patient's treating physician concludes, in the exercise of professional judgment, that the disclosure is in the patient's best interest and will either: 1) assist the person to whom the disclosure is made to assist with the patient's medical care (such as to pick-up prescriptions or medical supplies), or 2) assist in disaster relief efforts related to the notification of family and friends of the patient's location, general condition or death.

Access Request Processing

Actions to be taken for access

1. The, DCO has been appointed as SCNM's "privacy official". The privacy official will be responsible for receiving and processing requests by patients or their designated personal representatives to inspect or copy health information that pertains to these individuals.

2. The privacy official has met with the CMO to review the inspection procedures, including those relating to denial and subsequent review, and has incorporated those procedures in the forms for requesting and responding to requests for such access.

3. The privacy official has reviewed our professional liability carrier's guidance regarding inspection requests and procedures and these procedures comply with their guidance.

4. Instruct staff that requests for inspection or copying will be forwarded to the privacy official

5. Train staff to inform all patients or their personal representatives who request inspection or copying of their health information orally that they will be contacted by the privacy official within 2 days of the request. This contact will be to verify receipt of the request; it will be done by telephone. If privacy official is on vacation or otherwise absent, the designated alternate staff member who is responsible for answering voice mail will inform the patient that the matter will be addressed when privacy official returns from vacation.

6. At the initial contact, inform the patient or their personal representative that this practice requires the request be documented and submitted using our Request for Patient Access to Health Information form unless this has already been completed. This form will be mailed or faxed to the patient; if the patient expresses concerns about completing a form the DCO will offer assistance in its completion.

7. Verify identity of all requests when they are not from the patient, personal representative, or other person whose identity is not known. People who make requests in person or by telephone (who are not known, or the patient or personal representative) will be asked to mail or fax a written request to this office. Upon receipt the address and contact information will be verified. Governmental requests in person or by phone will be asked to mail or fax a written request to this office. Governmental officials

will also be asked to produce a badge or identity card and a call back number for confirmation. Upon receipt the address and contact information will be verified. This office will verify the identity of patients who call for information by a simple request for their date of birth. Calls for medical malpractice related requests will immediately be referred to our professional liability carrier. Medical board requests and governmental requests will also be forwarded to our attorney.

8. Track each request and the submission of the Request for Patient Access to Health Information on the Request for Patient Access Tracking Information form which is incorporated into the Request form.

9. Once the Request for Patient Access to Health Information form is received review the request form. Verify the scope of access requested (all records or a portion). Determine if the patient or their personal representative requires a) an inspection only, b) copies only or c) inspection and copies. Determine the records format requested. Review and "adjudicate" a request form within three (3) working days of receipt. DCO may call the patient or the patient's representative to discuss the scope, format or other aspects of the request to facilitate the timely provision of access.

10. Review the inspection request and determine if the request will be granted or denied. If a request is granted determine a convenient time (depending on scope of records requested for inspection) for inspection within 5 working days of receipt of the request.

11. Document the grant or denial of access on the Response to Request for Patient Access to Health Information form. Send the Response to Request for Patient Access to Health Information form by certified (receipt) mail.

12. Review requests for mental health records and minor's medical records to determine if such requests should be granted. **Mental health records do not have to be revealed to the patient if the DCO believe this would create a substantial risk of significant adverse or detrimental consequences to the patient, but at the patient's request these must be transferred to another mental health professional of the patient's choice.** The patient also has the right to have the decision reviewed by a third party. With respect to a minor's medical records, if the request is being made by a patient's personal representative, determine whether the practice should refuse to process the request as provided in the procedure on individual permission processing titled "Handling requests from personal representatives".

13. With respect to a minor's request for their own records determine whether the minor is entitled to access by virtue of their ability as an emancipated

minor, or by virtue of their ability to consent to the treatment reflected in the records.

14. If the request is being made by a patient's personal representative, determine whether the practice should refuse to process the request as provided in the individual permission procedure section titled "Handling requests from personal representatives".

15. If the request is made as a result of: a) a subpoena, b) an attorney's pre-litigation request, c) a law enforcement request, or d) any other request not made by the patient or the patient's, authorized personal representative follow the procedures as directed.

16. Unless the records are needed to appeal a denial of eligibility, this practice may charge for recreating the copies of the medical record.

17. If the request is for records copying or transfer, and this request is granted, arrange for this activity to be completed within 15 days of receipt of request and the prepayment by the patient or their personal representative.

18. Be present (on site) for approved inspection requests when the patient or their personal representative appears at the scheduled time. Be present at all times when the patient is reviewing any original records.

19. If the patient or their personal representative requests a review for mental health records which is denied, and the patient completes a request for transfer of these records by completing an additional Request for Patient Access to Health Information to another mental health professional, act on this request within three (3) days and ensure that any appropriate fees for the transfer are charged.

20. If the patient or their personal representative requests a review of a denied request for access to a patient's mental health records due to concern for the patient's safety, or for access to a minor's records due to concerns for the minor's safety, or for access to an incapacitated adult's records due to concern for the adult's safety, arrange for a review by either CMO, or another licensed health care professional in this practice who did not participate in the original review and denial.

21. Act on review requests that are documented in writing. Require the patient to complete a Request for Reconsideration of Denial of Access to mental health information, or minor's or incapacitated adult's PHI form and 2) Decision on Reconsideration.

22. Arrange for this review to be completed within 10 days of the receipt of the written Request for Reconsideration of Denial of Access to mental health information, Minor's or Incapacitated Adult's PHI form.

23. Document the results of this review on the Decision on Reconsideration of Denial of Access to mental health information, Minor's or Incapacitated Adult's Health Information form. Send to the patient by certified (receipt requested) mail and file in the central HIPAA compliance file

24. File all completed Requests and Responses in this organization's HIPAA Compliance file and not with the patient medical record.

Actions to be taken for access by correctional institutions and other law enforcement custodial situations

1. The DCO has been appointed as SCNM's "privacy official". The privacy official will be responsible for receiving and processing requests by correctional institutions and other law enforcement custodial situations.

2. Disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for:

    a. The provision of health care to such individuals;
    b. The health and safety of such individual or other inmates;
    c. The health and safety of the officers or employees of or others at the correctional institution;
    d. The health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;
    e. Law enforcement on the premises of the correctional institution; and
    f. The administration and maintenance of the safety, security, and good order of the correctional institution.

3. Document the name and identifying number of the correctional institution representative or law enforcement official requesting information of an inmate, the time of day of the request, and the verification that the information is required for the purposes described above in items a-f. Where possible, request this information in writing (and in an emergent situation via fax) to include the letterhead of the agency or organization requesting such information.

4. Track disclosures covered in this section by documenting them in the patient's chart.

Amendments or Addenda to Protected Health Information

Actions to be taken for amendments

1. The DCO has been appointed as SCNM's "privacy official". The privacy official will be responsible for receiving and processing requests by patients or their designated personal representatives to amend or add an addendum to their records.

2. The privacy official has met with the CMO to review the amendment and addenda procedures, and has incorporated these procedures in the forms for requesting and responding to requests for amendments or addenda.

3. The privacy official has reviewed our professional liability carrier's guidance regarding amendment requests and procedures and these procedures comply with their guidance.

4. Instruct all staff that requests for amendment will be forwarded tothe privacy official.

5. Contact all patients or their representatives who request an amendment or addenda orally within 10 days of the request. This contact will be to verify receipt of the request; it will be done by telephone. If privacy officialis on vacation or otherwise absent, an alternate staff member or privacy official assistant responsible for answering their voice mail will inform the patient that the matter will be addressed when the privacy official returns from vacation.

6. If the request is being made by the patient's personal representative, determine whether the practice should refuse to process the request as provided in the individual permission procedure titled "Handling requests for personal representatives".

7. At the initial contact inform the patient or their personal representative that this practice requires the request be documented and submitted using our Request for Amendment or Addenda form unless this has already been completed. Mail or fax the form to the patient; if the patient expresses concerns about completing the form, offer assistance in its completion.

8. Track each request and response and the submission of the Request for Amendment form and the Request for Amendment Tracking form using the Amendment or Addition Tracking Information form.

9. If the patient requests inspection of their health information in relationship to their request for amendment, advise them to complete a request for inspection as defined in the Access Request Processing procedure.

10. Review the proposed amendment information stated on the Request for Amendment or Addenda form. If the request is for an addenda go to step 11. If the request is for an amendment meet with the CMO to review the amendment and issue a determination within 15 days. The determination will either affirm or deny the amendment, consistent with the substantive grounds for denial set forth on the Response to Request for Amendment Form. Document this on the Response to Request for Amendment form.

11. If the request is for an addenda, and the requested addenda is no more than 250 words, insert it in the medical record and follow the procedure below for amendments.

12. Forward the grant or denial using the Response to Request for Amendment or Addenda form to the patient within 5 days of completion, by certified (receipt) mail.

13. At the direction of the CMO, forward a copy of the Response to Request for Amendment and the initial Request for Amendment to our professional liability carrier's risk management contact.

14. Upon determination of an approved addenda or amendment insert this amendment into the medical record (chart) and annotate the addition in the medical chart.

15. In the rare circumstance that the physician approves a correction to an original record, this will be done annotating the medical record with a new entry.

16. Upon approval of the amendment, a copy will be sent to the individuals or entities that the patient or their personal representative requested be notified. These will be sent by regular U.S. mail.

17. If the patient has NOT restricted notification to other individuals or entities we know received incorrect information, send a copy of the amendment to those individuals or entities as well. These will be sent by regular U.S. mail.

18. Within 10 days of approving an amendment notify appropriate staff of the amendment to ensure that accurate information is disclosed from this point forward.

19. If the patient responds to a denial by requesting either the disclosure of a "Statement of Disagreement" or a request that the original amendment request and denial be included with subsequent disclosures, notify the appropriate staff to add this information into the medical record (chart) in the "Amendments" section described above. If the patient submits a Statement of Disagreement (found in the Response to Rejection of Amendment Requests document), confer with the CMO to determine whether to prepare a rebuttal. The language of any such rebuttal should be reviewed by the organization's professional liability carrier or legal counsel before it is finalized. If a rebuttal is prepared, notify appropriate staff to include it with the "Statement of Disagreement," and send a copy by certified (receipt) mail to the patient.

20. File the original Request, Response, all Statements of Disagreement and related tracking information forms, as well as any further request by the patient in this organization's central HIPAA compliance file and not in the patient's file. Additionally, file any rebuttal in the medical record or chart in the "Amendments" section described above.

Restriction Request Processing

Actions to be taken for restriction requests

1. The DCO has been appointed as SCNM's "privacy official". The privacy official will be responsible for receiving and processing requests by patients or their designated personal representatives to restrict the uses or disclosures of health information that pertains to these individuals.

2. The privacy official has met with the CMO to review the restriction request procedures, including those relating to denial, and have incorporated these procedures in the forms for request, response and termination to the "Request for Special Privacy Protections" form.

3. The privacy official has reviewed our professional liability carrier's guidance regarding restriction requests and procedures and these procedures comply with their guidance.

4. Instruct all staff and members of the workforce that requests for special privacy protection will be forwarded to the privacy official or another designated staff member for handling.

5. Contact all patients or their representatives who request restriction of their health information orally within 10 days of the request. This contact will be to verify receipt of the request; it will be done by telephone. If privacy official is on vacation or otherwise absent, privacy official's alternate or assistant who is responsible for answering privacy official's voice mail will inform the patient that the matter will be addressed when privacy official returns from vacation. The initial contact will be to inform the patient or their designated personal representative that this practice requires the request be documented and submitted using our Request for Special Privacy Protections form, unless this has already been completed. Mail or fax this form to the patient; if the patient expresses concerns about completing the form, offer assistance in its completion.

6. Track each submission of the request for special privacy protections or response to Request for Special Privacy Protections Tracking Information form.

7. For requests made by a personal representative, determine if the personal representative is valid according to the individual permission procedure section titled "Handling requests from personal representatives".

8. Review the Request for Special Privacy Protections form upon receipt. This review will verify the scope of restrictions and compare these to the lists created of those items of protected health information we are capable or incapable of restricting use or disclosure. For request for restrictions, which do not appear on either list, consider the practical ability of the staff that would manage the restriction. Review and "adjudicate" a request form within 10 working days of receipt.

9. Document the grant or denial of the requested restriction on the Response to Request for Special Privacy Protections form. Send the Response to Request for Special Privacy Protections form to the patient or their personal representative by certified (receipt) mail. Document the date any restriction was granted in the space provided at the bottom of the Request for Special Privacy Protections form.

21. If the request is granted in full or in part, place one copy of the Request for Special Privacy Protections indicating those restrictions which have been granted and the date of that approval in the patient's medical record under a separate tab, or notation.

10. If the request is granted, meet with the appropriate workforce members to ensure that the request is implemented in their operational activities. Instruct the workforce to notify the privacy official immediately if they encounter problems implementing the restriction.

11. Act only on requests that are documented in writing. Require the patient to complete a new Request for Special Privacy Protections for any new or additional requests.

12. If the workforce encounters difficulty implementing any special restrictions, consider whether the restriction should be terminated.

13. Always terminate the restriction on the written request of the patient.

14. Document any termination of restrictions on the "Termination of Special Privacy Protections form", and send by certified mail (receipt) to the patient. The effective date of a termination by this practice shall be five (5) days after the termination notice is mailed to the patient, or a shorter time if the practice knows the patient has received the notice. Document this date in the space provided at the bottom of the Request for Special Privacy Protections form.

15. On the effective date of the termination, remove the Request for Special Privacy Protections form and any label alerting staff to the restriction from the chart and place, with a copy of the Termination of Special Privacy Protections form in this organization's HIPAA compliance file.

Actions to be taken for confidential channel requests

1. The DCO has been appointed as SCNM's "privacy official". The privacy official will be responsible for receiving and processing requests by patients or their designated personal representatives for "alternate" communications about their health information.

2. The privacy official has met with the CMO to review the request procedures, including those relating to denial, and has incorporated those procedures in the Confidential Channel Request form and the Response to Request for Confidential Channel Request form.

3. The privacy official has reviewed our professional liability carrier's guidance regarding alternate confidential communication channel requests and procedures and these procedures comply with their guidance.

4. Instruct staff that requests for confidential channels will be forwarded to the privacy official for handling.

5. Staff will ask patients or their personal representatives who request an alternate confidential communication channel to complete the "Confidential Channel Communication Request form. Train the front office or back office staff regarding the location of these forms and their responsibility to give the patient or their personal representative the form to complete. They will inform the patient that the privacy official will review the form.

6. Fax or mail a copy of the Confidential Channel Communication Request form to patients who were not given a form. If the patient expresses concerns about completing the form, offer to assist them in completion of the form.

7. Upon a request by a patient's personal representative, determine if the personal representative is valid according to the individual permission procedure section titled "Handling requests from personal representatives".

8. Based on available time, review the completed form while the patient is still present. If this is not practical inform the patient or their personal representative that that the privacy official will review the form and contact the patient within 5 days. If an alternate staff member is standing in for privacy official due to vacation or time off, inform the patient or their personal representative that the review may take 10 days. SCNM will

respond to such requests as soon as practical to minimize any risk of health information being communicated inappropriately.

9. Track each submission and response for confidential channel communication or response on the Confidential Channel Communication Request, Response and Tracking forms.

10. Reviews completed written requests and determine if the request is reasonable. Complete this by reviewing the existing PHI inventory "communication" list this organization has developed. Consider any request which does not appear on the list, and determine whether it can be accommodated. Grant reasonable requests, although this grant may be contingent on the patient's agreement to reimburse the practice for additional costs incurred to fulfill the request. Be certain to inform the patient of any reasonable costs associated with granting their request. Deny any request that this organization cannot reasonably accommodate. Document grants and denials on the Response to Confidential Channel Request form. Document the date any request is granted in the space provided at the bottom of the Confidential Channel Communications Request form.

11. Never ask the patient or their personal representative why the request is being made, train staff on this provision.

12. Respond with the grant or denial while the patient is still present if practical. The in person meeting will include providing the patient a copy of the Response.

13. If the patient is not present, within 5 days (10 days for vacation) of receipt of the written send by certified (receipt requested) mail a copy of the Response form.

14. Upon a grant of request, in whole or in part, place one copy of the Confidential Channel Communications Request form, indicating those restrictions which have been granted and the date of that approval in the patient's medical record under a separate tab, or annotation.

15. Upon grant of a request meet with the appropriate workforce members to ensure that the request is implemented in their operational activities. Instruct the workforce to notify the privacy official immediately if they encounter problems implementing the restriction.

16. Act only on requests that are documented in writing. Require the patient to complete a new Confidential Channel Communications Request for any revised, new or additional requests.

17. If the workforce encounters difficulty implementing any request for confidential channel communications, determine a practical method to comply with that request.

18. Document the date of any termination or change on the current Confidential Channel Communications Request form, which will be sent by certified mail (receipt requested) to the patient. Document this date in the space provided at the bottom of the Confidential Channel Communications Request form.

19. On the effective date of the termination or change, the Confidential Channel Communication Request form and any label alerting staff to a Confidential Channel Communication will be removed from the chart and placed, in this organization's HIPAA compliance file.

20. If the patient has submitted a new Confidential Channel Communication Request form, place one copy of the Confidential Channel Request form, indicating those restrictions which have been granted and the date of that approval in the patient's medical record under a separate tab. Affix a colored label to the front of the chart to indicate that an alternate communication channel is in effect. File an additional copy of the Confidential Channel Communication Request form in this organization's HIPAA Compliance file.

Disclosure Accounting Request Processing

Actions to be taken for disclosure accounting requests

1. The DCO has been appointed as SCNM's "privacy official". The privacy official will be responsible for receiving and processing requests by patients or their designated personal representatives for an accounting of disclosures of health information that pertains to these individuals

2. The privacy official has met with the CMO to review the disclosure accounting procedures, including those relating to denial and has incorporated those procedures in the forms for requesting and responding to requests for such disclosure.

3. The privacy official has reviewed our professional liability carrier's guidance regarding disclosure accounting procedures and these procedures comply with their guidance.

4. Routinely update all appropriate disclosures on SCNM's Tracking Accountable Disclosures Form.

5. Instruct staff to forward requests for disclosure accounting to you or another designated staff member.

6. Contact all patients or their personal representatives who request a disclosure accounting verbally within 10 days of the request. This contact will be to verify receipt of the request; it will be done by telephone. If privacy officialis on vacation or otherwise absent an alternate staff member will inform the patient or personal representative that the matter will be addressed when the privacy official returns from vacation.

7. Upon initial contact, inform the patient or their designated personal representative that this practice requires documentation and submittal of the request using the Request for Disclosure Accounting form unless this form has already been completed. Mail or fax this form to the patient; if the patient expresses concerns about completing the form they will be invited to visit the privacy official who can assist them in completing the form.

8. Once the Request for Disclosure Accounting form is received, review the request form. This review will verify that the accounting is valid and for health information disclosures where HIPAA requires an accounting. Review and "adjudicate" a request form within 10 working days of receipt.

9. If the request is being made by a patient's personal representative, determine whether the practice should refuse to process the request as provided in the procedure on individual permission processing titled "Handling requests from personal representatives".

10. Document the grant or denial of accounting in the response section of the Request Disclosure Accounting form. Send this response by certified (receipt) mail.

11. For granted requests where the practice requires additional time to prepare the Accounting, document this fact in the response section of the Request Disclosure Accounting form. Subsequently process the request within 90 days of the date of this form.

12. If this is a second request within twelve months of the original request, indicate in the response section of the Request Disclosure Accounting form that there is a charge for copying the records and preparing the accounting. The response will indicate the exact charge. Do not complete the accounting until the fee has been paid.

13. If the request is granted (or in the case of a second request in twelve months it is granted and the fee paid) prepare an accounting of disclosures. Compile the accounting by taking the information maintained on the Tracking Accountable Disclosures Form and transferring this to the

patient tracking log found at the end of each Request Disclosure Accounting form." Send this form by certified (receipt) mail. The accounting will be completed and mailed within 60 days of receipt of the Request for Disclosure form.

14. Track the communications related to the request and response on the tracking section of the Request Disclosure Accounting form. File Request forms in SCNM's HIPAA Compliance files.

Complaint Handling

Actions to be taken for all complaints received:

1. The DCO has been appointed as SCNM's "privacy official" to receive all privacy complaints and to take the appropriate action to resolve them

2. The privacy official has met with the CMO to review the complaint procedures, and has incorporated those procedures in the Complaint Concerning Protected Health Information form and the Response to Complaint Concerning Protected Health Information form.

3. The privacy official has reviewed our professional liability carrier's guidance regarding complaints and these procedures comply with their guidance.

4. Upon receipt of a verbal complaint by a patient (or personal representative), any member of the workforce who takes hears the complaint will inform the privacy official immediately. The information reported must include, at a minimum:

    - the name of the complainant;
    - the date and time of the complaint;
    - the substance of the complaint;
    - the name of the staff member who received the complaint.

5. Staff members will advise patients who make a complaint that this practice requires it in writing. Where possible, staff members will give the patient making the complaint a Complaint Concerning Protected Health Information form.

6. Contact the patient making the verbal complaint within 48 hours of receiving notice from the staff. Contact will always initially be done verbally, by telephone. Document the date and time of their response. If a voice mail is left, the privacy official will continue to pursue direct communication until it occurs. The voice mail message will not contain any details of the complaint.

7. Request that the patient complete a written Complaint Concerning Protected Health Information form. This form will be mailed or faxed to the patient; if the patient expresses concerns about completing the form request they are to come on site where the privacy official can assist them in completing the form.

8. Appoint an alternate staff member to handle complaints in the absence of privacy official during vacation, sick time or other time away from the practice. Advise staff regarding who has been appointed to perform these duties.

9. Respond to privacy complaints within 48 hours.

10. For complaints made by a personal representative, determine if the personal representative is valid according to the individual permission procedure section titled “Handling requests from personal representatives”.

11. File the completed Complaint Concerning Protected Health Information form in the HIPAA complaint form file and not as part of the patient’s medical record.

Actions to be taken when no compliance violation has occurred

1. Document these findings on the Complaint Concerning Protected Health Information form. (IMPORTANT: If, in the course of investigating the privacy complaint, privacy official determines that the complaint is related to clinical or medical care, the situation will be reported immediately to the CMO).

2. Meet with the patient and explain the findings; provide the patient with a written record of the complaint resolution using the Response to Complaint Concerning Protected Health Information form. The written record will be reviewed with any physician(s) concerned with the complaint and, may, if appropriate refer this matter to the practice's carrier.

3. Document the complainant's response (whether they are satisfied or dissatisfied with the disposition of the complaint) on the Complaint Tracking form.

4. If the patient is dissatisfied with the disposition of his or her complaint, refer this matter to the CMO, who in turn will report the matter as appropriate:

    - to our professional liability carrier as part of their early warning program;
    - to legal counsel.

Actions to be taken when a compliance violation has occurred

1. Upon determination that a probable violation of this organization's privacy policies has occurred, will meet with the physician to review the complaint and determine how to proceed.

2. If the physician concurs with the determination, consult with the organization's professional liability carrier or attorney and develop and document the violation and remediation plan.

3. Document the violation and remediation steps on the Response to Complaint Concerning Protected Health Information form as well as complete the Complaint Tracking Information form.

4. The tracking form and all other complaint forms shall be filed in the central HIPAA Compliance file.

5. Where a modification of a procedure or form would reduce the likelihood of a subsequent violation, such modification shall be made and reflected in the Notice or Privacy Practices if the change is material. Advise the appropriate workforce members or other persons (if any) who bear responsibility for privacy policy violations. Work with the appropriate manager to ensure that the appropriate sanctions are imposed on responsible personnel. (*IMPORTANT: If, in the course of investigating the privacy complaint, and the privacy official determines that the complaint is related to clinical or medical care, the situation will be reported immediately to the CMO who will in turn report this immediately to our professional liability carrier as an incident.)*

6. Meet with the patient and explain their findings; provide the patient with a written record of the complaint resolution using the Response to Complaint Concerning Protected Health Information.

7. If the patient is dissatisfied with the disposition of his or her complaint, refer this matter to the CMO who in turn will report the matter as appropriate:

   - to our professional liability carrier as part of their early warning program; and
   - to legal counsel.

8. Report to the physician partner in charge on a weekly basis the status of the remediation plan until all corrective activities have been accomplished.

Actions to Be Taken For All HIPAA Investigations

The Final HIPAA Enforcement Rule was published in the federal register on February 16, 2006. The enforcement rule establishes how the Department of Health and Human Services will investigate and enforce the HIPAA rules.

[Covered entities should be aware of a significant risk of penalties if they are found in violation and an agreement for corrective action does not occur. If the investigation results in a penalty, no matter how small, the following will occur:

- **Notification of the Public and other agencies upon a final penalty. This means that the Secretary of the Department of Health and Human Services *must* notify the public and certain agencies if you are assessed a penalty. This includes state and local medical or professional societies, utilization and peer review organizations, state and local licensing organizations, and so forth. Thus the notification can be more devastating that the possible penalty!**

Organizations should do everything within reason to informally resolve an investigation before it goes to a penalty phase. Be very careful that you respond to all subpoenas or written communication during an investigation. If the OCR or CMS is not able to informally settle the case they will alert you to the penalty phase. You have the right to request a formal hearing at this point!]

1. The DCO has been appointed as SCNM's "privacy official". The privacy official will be responsible for receiving and processing all HIPAA Investigations.

2. This medical practice has trained all staff, including physicians, to immediately notify the Privacy Officials upon receipt of a notice of a HIPAA investigation. The actual notification will immediately be forwarded to the Privacy Officials. If they are not available for more than three days (due to vacation or other kind of leave) the notification will be forwarded to their back-up or to the most senior management in place.

   Notice of an investigation may be received from the Office of Civil Rights (Privacy investigations), the Centers for Medicaid and Medicare Services (Security and Transaction Code Set violations), the Office of the Inspector General for the Department of Health and Human Services, or from the U.S. Attorney General's office. You may also receive notice from State agencies if they are investigating a violation of State regulations that parallel HIPAA.

3. Immediately upon receipt of notice of an investigation, review the contents of the notice and create documentation to record the steps completed in handling the investigation.

4. The Privacy Officials will meet with senior management (e.g. Medical Center Steering Committee and CMO, to review the contents of the notice. Determine if you will seek legal counsel before proceeding. [**Note: Consider the various resources available to assist in dealing with a HIPAA investigation. Also consider notification of the professional liability carrier.**

5. If the contents of the investigation notice are not clear, get in touch with the contact person listed on the notice from the Office of Civil Rights, or for a Security or Transaction Code Set investigation, from the Centers for Medicaid and Medicare Services. Ask for any clarification regarding the nature of the violation they are investigating. [**Note: Generally, OCR or CMS will not disclose information about the identity of the person who may have made the complaint leading up to the investigation. Sometimes an investigation will take place without a specific complaint. However, the privacy official may be able to obtain clarification regarding the investigation that can help in the internal review and follow-up. Additionally, making contact will ensure that the investigating agency knows the privacy official has received the notice and are interested in cooperation. The investigative agencies have established that they are also interested in assisting covered entities in determining corrective actions.]**

6. Begin an internal investigation to review the incident. [**Note: If there is a compliance committee, immediately convene a committee meeting to establish procedures and ownership of the investigation. Depending on your internal procedures, include the investigation issue to your E.V.P.]**

7. Notify any staff members who may be part of the review that privacy official is investigating a possible HIPAA violation and their cooperation is needed. Reiterate that their cooperation with the privacy official or the HHS agency will not result in any retaliation against them.

8. Throughout the internal investigation and any subsequent investigations by authorities, **do not** threaten, intimidate, coerce, harass, discriminate against, or take any other retaliatory action against any individual who is either a member of the workforce or who may have made a complaint. This is specific to a person filing a complaint, testifying, or participating in the investigation or hearings. Ensure that any staff members involved have been notified of this requirement.

9. Document theinternal investigation including any interviews with staff members. If it is determined a violation has occurred or a gap in compliance exists, immediately correct this gap with corrective measures and document how this has beendone.

10. Conduct a training of all workforce involved to ensure they understand the nature of the violation and gaps and how these are being corrected . Reiterate current sanctions policies for failure to follow HIPAA policies and procedures.

11. If a member of the workforce has violated policies and procedures, follow current sanction procedures. Be sure that the sanctions are well documented and cannot be construed as retaliation. (**Note: This is a very sensitive issue and may require good legal counsel before proceeding).**

12. Meet with the investigating agency to review findings and cooperate with them if they choose to conduct their own investigation. If a violation has occurred, share with them the corrective actions and solicit their approval.

    If not able to come to immediate agreement with the investigative agency, be certain to request an appeal *prior* to penalties being imposed.

HIPAA Compliance Records Retention

1. The DCO has been appointed as SCNM's "privacy official". The privacy official will be responsible for ensuring that HIPAA compliance records are retained per Arizona State Law.

2. The privacy official has met with the CMO and reviewed these procedures.

3. The privacy official has reviewed the HIPAA guidelines regarding records retention and has created an inventory of the kinds of records per Arizona State Law.

4. The privacy official has reviewed our professional liability carrier's guidance regarding records retention and these procedures comply with their guidance.

5. Annotate the front cover of all files in this organization's HIPAA compliance file. Ensure this file system has been established according to the procedure on "setting up the HIPAA Central File".

6. Stamp any related record that is not filed in this organization's HIPAA compliance file with the above mentioned stamp. Remember, however, that the six year time frame runs from the date the document was created, or was last in effect, whichever is later.

7. Periodically, review the HIPAA compliance file and ensure that all file covers are appropriately stamped.

8. Starting on April 15, 2009, periodically review the files and destroy (by shredding or other means) and discard those records that do not need to be retained (provided guidance from our professional liability carrier, legal counsel or state law does not suggest or require a longer retention period).

Minimum necessary access, request and disclosure

Actions to be taken for minimum necessary access, request and disclosure:

1. The DCO has been appointed as SCNM's "privacy official". The privacy official will be responsible for establishing and maintaining procedures related to minimum necessary access, request and disclosure.

2. The privacy official has met with the CMO to review the minimum necessary access, request and disclosure procedures.

3. The privacy official has reviewed our professional liability carrier's guidance regarding minimum necessary access, request and disclosure procedures and these procedures comply with their guidance.

4. Implement chart organization procedures that separate information which generally should not be disclosed as a routine matter such as psychotherapy notes, HIV test results, confidential communication from third parties, litigation records which are not patient records, and public health disclosures and relevant information (discussions of abuse, etc.).

Minimum Necessary Access

1. Complete and maintain an up to date listing of staff and their job descriptions. Each job description will be mapped to the PHI inventory.

2. Ensure that staff and workforce training and orientation include identification of the PHI access required for each job function. Staff will be advised to limit their access to their job description and warned of the sanctions for violating this procedure.

3. Where applicable, implement technical controls for electronically maintained PHI to provide access based on job description and function.

Disclosures by this practice

1. Initially and periodically review our PHI inventory and determine those items that typically are "disclosed" on a routine and recurring basis, other than for treatment purposes. This review has also identified how these items can be minimized in their disclosure and a standard protocol has

been established to limit disclosures to the amount reasonably necessary for the purpose of these routine and recurring disclosures.

2. Initially and periodically review the list of PHI that is typically disclosed on a non-routine basis other than for purposes covered by an authorization. Evaluate and handle all requests for disclosures that are non-routine to ensure that the disclosure is appropriate and the minimum needed to accomplish the purpose required. This organization considers non-routine requests inclusive but not limited to those required for an HHS compliance review, public purposes and law enforcement where there has been no admission of a violent crime. However, for an HHS compliance review minimum necessary does not apply.

3. Periodically meet with staff to establish controls on records and information release. Review all records releases subject to an authorization or for non-routine purposes.

4. Determine that a valid authorization is in effect for disclosures covered by an authorization on file. Upon validation, disclose the records according to the specifics of the authorization only.

5. Review all requests from law enforcement. Determine if these records include admissions about a violent crime; if this is the case limit the disclosures to those specified in CFR 164.512(j)(3).

6. Do not disclose the entire medical record unless the entire medical record is specifically justified as the amount of information needed to accomplish the purpose of the use, disclosure or request.

Requests by this practice

1. Initially and periodically review the PHI inventory for this organization and determined the PHI typically requested for this organization's payment and healthcare operations. Establish standards for the information required for these purposes.

2. Periodically meet with both the front and back office staff and train them on the need to conform routine requests for PHI to the standards defined in item 1.

3. Train front and back office staff to forward all contemplated requests for PHI considered non-routine to privacy official's attention. Review each request and ensure that the information this practice requests is only the minimum needed to accomplish the purpose of the request.

Notice of Privacy Practices and Acknowledgement

Actions to be taken for notice and acknowledgement:

1. The DCO has been appointed as SCNM's "privacy official". The privacy official will be responsible for establishing and maintaining a notice of privacy practices and acknowledgement procedure.

2. The privacy official has met with the CMO to review the notice and acknowledgement procedures, and have incorporated those procedures in the Notice of Privacy Practices and Acknowledgment form.

3. The privacy official has reviewed our professional liability carrier's guidance regarding notice and acknowledgement procedures and these procedures comply with their guidance.

Publication of the notice

1. Create a notice of privacy practices.

2. Use the MS Word footnote feature to indicate the date the notice was created.

3. Retain all versions of the notice in the central HIPAA file. New versions supersede any previous notice.

4. Post the notice in the waiting room. Do this by keeping three laminated copies of the first part of the layered notice on clip boards, attached to hooks on the [east] wall of the waiting room.

5. Also keep one copy in a laminated form in a "stand" on the receptionist counter top. This version will be the complete notice.

6. Reproduce 25 copies of the full notice available and keep this inventory on hand at the front desk. This inventory will be used when a patient requests a copy of the notice to take with them.

7. Produce a version of the notice in other languages commonly spoken by the patient of this practice.

8. As of the compliance date, April 14, 2003 train the front desk and ensure that all patients (new and established) who have not previously been given

the notice will be provided the notice after they check in for their office visit and request they sign the acknowledgement. This will be accomplished in this practice by providing each patient with a clipboard containing the notice and the acknowledgement form.

9. Meet with the front desk and scheduling staff to ensure that patients who need to receive the notice and sign an acknowledgement are advised to arrive twenty minutes early for their scheduled appointment.

10. Upon each change in the notice, post the most current notice in the waiting room (and on the practice's website) and replace the copies at the front desk. The revised notice will thus be available for patients at each appointment. Upon request give each patient the revised notice. If they request a copy to take home, allow them to take this copy. Indicate the date the former notice was superseded, and place this copy of the note in the HIPAA compliance file.

Acknowledgement

1. Train the front desk to give each patient who receives the notice a copy of this organization's Acknowledgement of Receipt of Notice of Privacy Practices. The Acknowledgement is a separate page that is attached to every notice.

2. Train the front desk to file the patient's signed acknowledgement in the patient's medical record under a separate tab.

3. Train the front desk to contact the privacy official or replacement if the patient refuses to sign the acknowledgement. Immediately meet with the patient to answer any questions or concerns.

4. Never condition treatment on refusal to sign the acknowledgement.

5. If the patient continues to refuse to sign the acknowledgement document, two staff members will annotate with their signature and annotate the patient refused to sign.

6. Patient's initially seen by the physician in the emergency room or at the hospital will be covered by the hospital's notice. However, upon their first visit to this practice train the front desk to provide a notice and asked to complete the acknowledgement.

7. Train the front desk to recognize patient concerns or issues with the notice. Specifically the front office will understand that the presentation of the notice is a time when a patient may request special privacy

protections, alternate confidential communication channels, request to amend PHI, disclosure accounting, or inspection or copying of PHI. Instruct all to forward such requests to the privacy official or other designated staff.

Workforce training and awareness

Actions to be taken for workforce training:

1. The DCO has been appointed as SCNM's "privacy official". The privacy or security official will be responsible for establishing and maintaining a workforce training and awareness program. The privacy official will identify the training resources appropriate for this organization.

2. The privacy or security official has met with the CMO to review the training and awareness procedures.

3. The privacy or security official has reviewed our professional liability carrier's guidance regarding training and awareness procedures and these procedures comply with their guidance.

4. Complete and maintain an up to date listing of staff and their job descriptions. This will include temporary office staff, locum tenens and physicians and any other members of the workforce. Each job description will be mapped to appropriate privacy and security policies and procedures. Log this information on the Job Responsibilities with Respect to PHI form.

5. For training purposes use an up to date quick training reference guide using a) the PrivaPlan PowerPoint Kickoff and User's training materials, b) the HIPAA Ready Reference, c) PrivaPlan Stat, d) the Privacy and Security Policy Drafts and this Procedure Manual, and e) the HIPAA Rule Training booklet.

6. Make entries for each training session in the workforce training log.

7. Conduct an initial HIPAA with all newly appointed staff members.

8. Each existing member of the workforce will complete the quiz in the HIPAA Rule Training booklet. This includes signing the certification statement and completing the job responsibility sheet.

9. The Privacy or Security Official will grade all quiz responses. A pass score requires answering all questions correctly. This is noted on the quiz form.

10. Workforce members who do not pass the quiz will be retrained and retested until they do pass.

11. Ensure that all new staff as well as temporary staff will have a basic orientation in the policies and procedures related to their job function. This training will use the quick reference guide, the relevant policy and procedure taken from the Policy draft and this Procedure manual, and for new staff the HIPAA Rule Training booklet. Ensure that all new management or new providers receive this training.

12. Ensure all new staff understands SCNM's computer, internet and email use policies and have signed to this effect.

13. New staff must complete HIPAA training within 30 days of their start date. New staff must complete the online training provided by SCNM.

14. Include a HIPAA awareness-training component in monthly staff meetings. To maintain awareness and increase understanding, at each meeting and on a rotating basis, one privacy and one basic security topic will be reviewed. The topic list will include patient rights and SCNM's obligations.

15. At the regular staff meetings, review any recent patient requests for a) special privacy protections, b) alternative confidential communication channels, c) amendments or d) disclosure accounting with the appropriate staff. Review any recent problems with access requests.

16. Review all patient privacy and security complaints with the workforce within 30 days of resolution of each complaint. This will be a separate training meeting and not combined with any other training.

17. At the regular staff meetings review any recent security incidents (using the security incident form), or revisions to the risk analysis and the Risk Analysis Tracking Form as a result of new evaluation or audit information. At these meetings, the security official will update staff on new virus and worm threats as well as any other security changes including physical security violations or changes.

18. The security official will also review alerts or news items from the press, our computer system vendor, and other sources.

19. The security official will assess these alerts and develop an email and/or printed memorandum to be distributed alerting workforce members

(including the physicians) about these new threats and reminding all workforce to keep antivirus software up-to-date.

20. Periodically, the security official will also use these memorandums to remind workforce members about this organization's other security policies and procedures, especially after an incident or breach.

21. Train each member of the workforce to not share their passwords or user ID's and to change them according to this organization's procedure. Train each staff member to use strong passwords that are a combination of numbers and letters, at least 6 characters long and not a variation of a previous password.].

22. Train each member of the workforce who has access to electronic PHI to log off whenever they are away from their computer for prolonged periods of time.

23. Train staff to use the security incident reporting forms whenever a suspected or actual security incident occurs. Train staff to recognize a security incident, including sudden system performance changes, notification that a file has been corrupted or infected by a virus, and other incidents.

24. Train staff to not download suspicious email messages, attachments or software or to bring media (CD ROMs, diskettes) from home and download on the network.

25. Train staff to notify the security official whenever they receive a message regarding a security update that is ready for installation or follow the procedure to run all security updates. Train staff to maintain antivirus, spyware, and other malicious software protection updates and to never disable these features and protections without approval from the security official.

26. Train staff to keep all alarm system access codes confidential and to always ensure that doors are locked at night and alarms set.

27. Maintain the Workforce Training Log.

28. File the Workforce Training Log and the HIPAA Rule Training booklet certifications in the HIPAA records filing system central file.

Sanctions

Actions To Be Taken For Initially establishing HIPAA sanctions

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. THE DCO HAS REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS TO THE GUIDANCE PROVIDED BY OUR PROFESSIONAL LIABILITY INSURANCE CARRIER, EMPLOYEE PRACTICES CARRIER, STATE AND FEDERAL LAW AND GUIDANCE FROM OUR ATTORNEY. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT the DCO BEFORE CONTINUING.

2. The privacy and security official has reviewed the HIPAA privacy and security procedures and policies of SCNM and determined the kinds of violations that might occur and prioritized them by level of severity.

3. The privacy and security official has reviewed existing sanctions if any that are in place.

4. The privacy and security official has developed a series of sanctions that correspond to the HIPAA policies and procedures of this organization and the level of severity.

5. The privacy and security official has updated this organization's employee manual and has included the revised sanctions.

6. The privacy and security official has included a specific computer, internet and email use policy in this organization's employee manual. [Note: It may be helpful to include a specific policy statement in the manual and have employees or other members of the workforce sign that they have read it. A sample template is included under Document Templates.

7. The privacy and security official has included sanction training in all new employee training and for periodic training updates.

8. The security official will review all incident reports and other notices of breach according to the Security Incident response and reporting procedures. The security official will apply sanctions to any member of the workforce who breaches the security policy.

9. The security official will document the sanction applied and the outcome in the personnel file of the workforce member.

10. The security official will address actual violations immediately based on the nature of the violation. This may include activating the contingency planning procedure in this manual, the sanctions procedures or other relevant procedures.

11. In the event of a malicious action by a present or former employee or an outside individual, the security official will immediately meet with the CMO, and together they will seek their attorney's advice for further actions. They will also contact the professional liability carrier and, if applicable, the employee practice's carrier

12. The privacy and security official has included training on SCNM's protection for whistleblowers.

13. The privacy and security official will routinely review privacy complaints or security incidents to determine if sanctions should be strengthened or modified. The privacy and security official will subsequently revise sanctions (if appropriate) and notify staff via training and new employee manuals.

Business Associates

Agreements

1. This organization has inventoried all outside business and service vendors to determine if they are business associates.

2. This organization has implemented business associate agreements as of the compliance date.

3. This organization has used business associate agreements that contain required HIPAA language and terms.

4. This organization has sent the Business Associate agreement addendum to any existing business associate who signed an agreement prior to the security rule effective date (April 20, 2005).

5. This organization has customized each agreement to reflect the actual uses and disclosures of either PHI or electronic PHI by the business associate.

6. This organization has modified all underlying agreements with business associates to allow for immediate termination based on a violation or to concur with other aspects of the HIPAA requirement.

7. This organization has discussed the requirement for the business associate to safeguard PHI or electronic PHI in the same manner as the organization does. This includes activities by the business associate with agents and subcontractors that it might use.

8. These steps will be repeated with each new business associate.

Actions to be Taken for Ongoing Business Associate Management

1. If the Privacy or Security official learns of an activity or pattern that shows the business associate has breached the agreement, they will immediately notify the business associate in writing and request reasonable steps to cure the breach or end the violation.

2. For severe violations, the Privacy or Security official will terminate the agreement.

3. If the business associate is unable or unwilling to cure the breach or end the violation, the agreement will be terminated. If the termination is not feasible due to an underlying agreement, the breach or violation will be reported in writing to the Secretary of the Department of Health and Human Services.

Security Procedures

Security Official Job Description

Actions to be taken for the Security Official Job Description

1. The DCO has been appointed as SCNM's "security official". The security official and the Medical Director will be responsible for completing the job description for the security official.

2. The security official has met with the <insert name of management> to review the HIPAA Security rule and to determine the responsibilities of the security official.

3. The CMO has agreed to the following job description.

SECURITY OFFICIAL JOB DESCRIPTION

Security Official; The DCO

Job-Sharing? Yes—this job is performed by the DCO who is also the Privacy Official

Job Description:

The security official is responsible for implementing and maintaining SCNM's HIPAA Security requirements.

Reporting structure:

The security official reports directly to the EVP.

Job Duties

1. Complete the risk analysis and periodically review and revise.
2. Assess the threats to electronic PHI
3. Implement safeguards to minimize these threats and periodically monitor these safeguards to be sure they are working. This will encompass both technical and non-technical issues.
4. Implement contingency plans such as emergency mode operations (finding alternate locations to run critical applications like billing, appointment scheduling or electronic medical records.

5. Implement the data back-up process, including identifying who will take back up tapes off site.
6. Maintain and periodically check the back-up process including ensuring tapes are taken off site, and not damaged in transit.
7. Manage the restoring data when the system fails and the most recent back up is needed or during emergency mode operations.
8. Manage access authorization (passwords, user ID's) for all applications and systems and for all workforce (includes granting access, changing access privileges, terminating privileges and access).
9. Coordinate (with the human resources person, office manager or other appropriate party) workforce clearance procedures for all new hires and for existing staff who may require increased privileges (if applicable).
10. Implement and manage physical safeguards (or coordinate with Privacy Official if separate personnel).
11. Implement and manage administrative safeguards (or coordinate with Privacy Official if separate personnel).
12. Implement security incident reporting.
13. Respond to security incident reporting including investigating incidents and if necessary correcting vulnerabilities (mitigation).
14. Review business associates and implement business associate agreements with business associates who use electronic PHI or coordinate with Privacy Official if separate personnel).
15. Implement workforce sanctions for members of workforce who violate this organization's security policies and procedures (or coordinate with Privacy Official if separate personnel).
16. Implement workforce security training and awareness and maintain training programs (or coordinate with Privacy Official if separate personnel).
17. Ensure all new hardware that is connected to the existing system is secure (virus free, has all security programs running and so forth).
18. Ensure that all new software applications that are installed on the existing system, or will interface with the existing system is secure (virus free, has security features installed such as passwords).
19. Maintain version control (downloading security patches, updating virus and firewall software).
20. Manage user identification and authentication systems that are software, hardware and password related.
21. Manage the information systems activity review procedures and audit procedures.
22. Ensure ePHI integrity.
23. Ensure appropriate encryption or protection of any ePHI that is transmitted.
24. Routinely evaluate security and audit processes. Keep triggering events chart (HIPAA Ready Reference) up to date.

Risk Analysis and Risk Management

Actions To Be Taken to Conduct and Maintain a Risk Analysis and for Risk Management

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. THE DCO HAS REVIEWED THIS PROCEDURE.

2. The security official has reviewed this organization's prior risk analyses (if any); based on this review the security official has developed a plan for a current risk analysis. **Note:** If privacy official has recently completed a risk analysis, for example as part of a disaster recovery plan or part of SCNM's facility emergency plan, it may provide a substantial amount of assessment data.

3. The security official and senior management has determined that a risk analysis will be performed.

4. The security official has documented the risk analysis using the Risk Analysis Tracking form.

5. The security official has reviewed the risk analysis with the practice management software vendor and incorporated their suggestions.

6. The security official will modify the risk analysis and the accompanying Risk Analysis Tracking Form whenever a) new software or hardware is implemented, b) a new job responsibility or function is created, c) based on security incidents that reflect a new threat or vulnerability, d) awareness of a new threat, vulnerability or probability of a threat or e) a new physical location or change in physical location.

7. The security official will review the risk analysis and update if appropriate annually. The risk analysis will include both technical and non-technical safeguards.

8. Based on periodic review of the risk analysis, or updates the security official will modify the procedures to ensure that any new threat or increased probability of a threat is covered by a sufficient security measure.

9. This security official will ensure that the anti-virus software is updated on all workstations and the automatic live update feature is enabled. Periodically, the security official will review this.

10. The security official will ensure the firewall is enabled on all workstations and enabled to the highest level of protection. [Highest level will shut down some systems; allow flexibility.] The security official will periodically review the firewall protection with the hardware vendor to ensure it is compatible with the network firewall in the network router.

11. The security official will review all security update notices from the operating system vendor and the application system vendors. These will be installed as soon as practicable.

Information Activity and Systems Review

Actions to Be Taken to conduct and maintain information systems review

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. The DCO HAS REVIEWED THIS PROCEDURE.

2. The security official will immediately review any security incident report and follow up on suspected or actual violations.

3. The security official will run the anti-virus scans, spyware scans, and data integrity scans (if applicable) on a weekly basis and determine if there are infected or corrupted files.

4. If the security official determines there are infected or corrupted files, they will contact the vendor if the files relate to the practice management or appointment scheduling system, or follow the anti-virus, spyware, or data integrity software recommendations for other files.

5. On a weekly basis SCNM will review the firewall security report to determine if there has been attempts to penetrate the information system that are not authorized.

6. The security official, working with the vendor, will enable both application and operating system level event audit tools that record system access by date, time of day, User ID and file or program.

7. On a weekly basis, SCNM will review the event audit report; the security official will focus on unusual time of day access by authorized persons, or attempts using invalid or obsolete passwords.

8. The security official will pay special attention to access attempts by recently terminated employees.

Workforce Security

Actions to Be Taken to Clear Employees for Access to Protected Health Information

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. The DCO HAS REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS TO THE GUIDANCE PROVIDED BY OUR PROFESSIONAL LIABILITY INSURANCE CARRIER OR YOUR EMPLOYEE PRACTICES CARRIER. ALL APPLICABLE STATE AND FEDERAL LAWS REGARDING DENIAL OF EMPLOYMENT FOR A CLEARANCE FAILURE ARE FOLLOWED. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT THE DCO BEFORE CONTINUING.

2. The security official using the risk analysis will a) ensure that references were checked for staff accessing non-critical applications and b) background checks have been done for employees accessing critical applications.

3. The security official and the CMO, using guidance from the professional liability carrier, the employee practice's carrier, and state and federal law will determine when an employee's application for employment is to be denied due to the background check or reference check results and the job responsibilities this applies to.

4. If appropriate, the security official will run a background check using the web-based tool this office has implemented as appropriate. [**Note:** Ensure background checks or similar workforce clearance procedures are harmonized with existing human resource policy and conform to all state and federal laws such as EEOC, FLSA and FCRA.]

5. SCNM will review the results of the background check or the reference check. For checks that do not pass the criteria decided in step 3, the applicant will be denied employment or denied employment or denied the job responsibility applicable. State and Federal laws will always be adhered to.

6. This same process will be followed for existing employees or members of the workforce who are being assigned job responsibilities that involve data that has been defined as critical and requiring a background check. If the

background check results in a failure to meet the criteria, the security official and CMO will not reassign the employee and will consult with appropriate counsel regarding employment practices for this employee.

7. If the background check provides clearance, SCNM will assign the appropriate rights and privileges via password control, user ID and system privilege. The security official will also ensure that the physical access safeguards are implemented by providing applicable keys, access codes or pass cards and ID badges.

8. The security official will ensure that electronic PHI access control via the electronic information systems is always a combination of passwords, system user ID's and log-ons and system level privilege.

9. The security official will ensure that electronic PHI access control is where possible granted based on the role or job description with respect to PHI.

10. The security official will ensure that access control is in place for the diagnostic equipment used by this practice that contains electronic PHI.

11. The security official will ensure that the fewest number of employees possible are given administrator level access, or access to all files and systems.

12. The security official will ensure that password protection is in place on the PDA's and any other remote device used by the physicians and other workforce members.

Actions to Be Taken to Terminate Employees' Access to Protected Health Information

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. THE DCO HAS REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS TO THE GUIDANCE PROVIDED BY OUR PROFESSIONAL LIABILITY INSURANCE CARRIER, OR OUR EMPLOYEE PRACTICES CARRIER. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT DCO BEFORE CONTINUING.

2. The security official will review the circumstance requiring termination to assess whether the employee has been terminated or is changing job responsibilities.

3. Upon termination, SCNM will immediately remove the employee's user ID, passwords and system privileges. All remote access privileges will also be disabled including unique addresses (for example if the employee uses their own device), or blackberry or other addresses. All email accounts will either be disabled or forwarded to an alternate address.

4. Upon termination, the security official will immediately retrieve any mobile computer or device such as a PDA or laptop. The security official will ask for and retrieve any back up media such as zip disk, CD's, floppy disks, flash memory cards or memory sticks that contain ePHI , or any other sensitive information related to the practice. If these devices are the property of the individual being terminated, the security official will require evidence that the devices have been sanitized of all practice information or ePHI.

5. Upon termination, the SCNM will immediately change the security alarm access code and notify all existing employees of the new access code. (Note: if a pass card system is used, delete the pass card access. This assumes that the terminated employee has also returned all keys in their possession.)

6. Remind the departing employee of his/her continuing responsibility to protect sensitive information with which he/she has come in contact during his/her period of employment.

7. Update the job responsibilities with respect to PHI form and other logs that are maintained of employees/workforce members and their access.

Actions to Be Taken to Provide and Maintain Employees' Access to Protected Health Information

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. THE DCO HAS REVIEWED THIS PROCEDURE. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT DCO BEFORE CONTINUING.

2. The security official has met with the network vendor and our practice management and electronic medical records vendor to determine the best way to manage passwords.

3. The security official has reviewed the risk analysis and determined a password management program.

4. The security official has met with the CMO and other management to ensure their awareness and adherence to these procedures.

5. The security official will evaluate any new information systems or equipment that maintains, stores, creates or transmits electronic PHI and he/she will develop passwords, user ID/log-ons and system privilege codes if appropriate.

6. The security official will assign existing employees and workforce members appropriate access based on this analysis.

7. The security official will ensure that access is always a combination of passwords, user ID's, and system level privileges. Additionally, the security official will maintain the job responsibility with respect to PHI document and use this to apply or deny additional application or data specific access (based on the role of the employee or member of the workforce).

8. The security official will ensure that all passwords are changed regularly.

9. The security official will ensure that the fewest number of employees possible are given administrator level access, or access to all files and systems.

10. The security official will ensure that access is also mapped and restricted to the appropriate domains and server files and folders and, if appropriate, that these have password protection.

11. The security official will immediately, or as soon as practicable, delete any password that has been shared with any workforce member either

maliciously, unintentionally, or during emergencies out of necessity. A new password will be assigned.

12. The security official will insure SCNM keeps a written record of all passwords, or maintains a process by which new passwords may be assigned.

13. When an employee changes their job responsibilities, the security official will review the change. Where appropriate, if the change results in a reduction of responsibilities or access, the security official will modify the password and system privileges for the appropriate applications and data to restrict access. Where the change requires new access or increased access, the security official will modify the password and system privileges for the appropriate applications and data to allow access. These changes will be noted on the Job Responsibility with respect to PHI form.

14. The security official will determine if the change in job responsibilities will require decreased facility access. If so, the appropriate keys will be returned, and/or access codes or pass card code changes made. If the change will require increased facility access, the appropriate keys and and/or access codes or pass card codes will be provided.

Isolating Clearinghouse functions

Actions to Be Taken To Isolate Clearinghouse functions

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. THE DCO HAS REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS TO THE GUIDANCE PROVIDED BY OUR PROFESSIONAL LIABILITY INSURANCE CARRIER OR INFORMATION SYSTEMS VENDOR. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT DCO BEFORE CONTINUING.

2. The security official has met with the executive in charge and other management to ensure their awareness and adherence to these procedures.

3. The security & privacy official have worked to assess and inventory the healthcare clearinghouse functions.

4. The security & privacy official has worked to complete a thorough PHI inventory as well as a formal risk analysis.

5. The security official has evaluated the ePHI that is vulnerable to use or disclosure by unauthorized persons or entities who are members of the workforce of the “larger” organization.

6. The security official, working with the privacy official, has identified all users and entities that need access to ePHI for healthcare clearinghouse functions, and mapped this according to role, using the Job Description with respect to PHI form. The security official working with human resources and the privacy official maintains this form on an ongoing basis. Human resources immediately notifies the security official of all new hires, terminations, or job changes.

7. The security official has developed appropriate role- and user-based password and authentication to ensure access is limited to appropriate members of the workforce

8. The security official has reviewed the applications and network architecture and has established separate servers for the healthcare clearinghouse

9. SCNM has updated the pass key access codes (and will maintain these) to the location of the healthcare clearinghouse activities to restrict physical site access to appropriate members of the workforce of the larger organization.

10. SCNM ensures that the data backup for the healthcare clearinghouse that is done by the larger organization's IT department is a separate data tape. This tape is sent offsite to the remote data vault but is always logged and tracked separately from the back up media of the larger organization.

11. The security official has developed a separate set of policies and procedures and training materials (and keeps these up to date) for the workforce of the healthcare clearinghouse.

12. The security official has conducted training for the healthcare clearinghouse workforce and maintains training, periodic reminders, security alerts and all other components of the larger organization's security policy and procedure.

Malicious Software Protection

Actions to Be Taken To Develop and Maintain Malicious Software Procedures

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. THE DCO HAS REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS TO THE GUIDANCE PROVIDED BY OUR PROFESSIONAL LIABILITY INSURANCE CARRIER OR INFORMATION SYSTEMS VENDOR. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT DCO BEFORE CONTINUING.

2. The security official has met with the CMO and other management to ensure their awareness and adherence to these procedures.

3. The security official has reviewed the risk analysis and determined risks associated with malicious software as well as the appropriate measures to reduce these risks.

4. The security official, using the electronic protected health information inventory, has identified all programs, computers, and other devices that must be guarded against malicious software.

5. The security official has met with the network vendor and our practice management and electronic medical records vendor to determine the best way to guard, detect, and report malicious software.

6. The security official has implemented the following software: antivirus software, spy-ware, and firewall software. The security official has ensured that the automatic live update feature is enabled on all workstations for this software. The security official has ensured that the software is enabled for all appropriate applications.

7. The security official has ensured this software is enabled on any device that may be connected from time to time to the network, including physician's personal laptop, or other portable devices.

8. The security official has trained all staff to never disable these software programs.

9. The security official has trained all staff not to open email attachments from unknown parties, suspicious email messages, or any attachments or emails that are not expected.

10. The security official has trained all staff on this organization's policy that email and computers must NEVER be used for personal correspondence or matters.

11. The security official has trained all staff not to download any items, and that this organization forbids web browsing for any matter not related to business, and specifically forbids web browsing pornographic sites.

12. The security official has trained all staff not to download any CD-ROM, DVD, MP3 file, floppy disk, or other media that is personal or in a not related to their job responsibilities. All staff must obtain the security official's approval before downloading any media.

13. The security official has trained all staff that it must follow these procedures whenever a device such as a laptop or home computer is used for business purposes and will subsequently be connected to the office network.

14. The SCNM will only download and install software from trusted sources where a bona fide purchase has occurred from the software manufacturer or a legal reseller.

15. The security official will only download and install software updates from trusted sources as in item 14 above.

16. The security official will run anti-virus and spy-ware detection scans on the network server and all workstations every week. Malicious software that is detected will be quarantined.

17. The security official will follow all password management, log in, termination, and related procedures to limit the ability of unauthorized persons or persons with malicious intent to introduce malicious software.

18. The security official has determined that passwords will be changed every 90 days except in the case of termination or job change when the password must be deleted or changed immediately.

19. The security official will document all detection of malicious software on this organization's security incident report and follow reporting procedures.

Log-in Monitoring

Actions to Be Taken To Develop and Implement Log-in Monitoring

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. THE DCO HAS REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS TO THE GUIDANCE PROVIDED BY OUR PROFESSIONAL LIABILITY INSURANCE CARRIER OR INFORMATION SYSTEMS VENDOR. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT DCO BEFORE CONTINUING.

2. The security official has met with the CMO and other management to ensure their awareness and adherence to these procedures.

3. The security official has reviewed the risk analysis and determined that log-in monitoring is focused on log -in attempts and discrepancies.

4. The security official has met with the systems vendor of a) the network and the network operating system, b) the practice management and electronic medical records system [Note: insert additional applications as needed] to review the scope of monitoring.

5. The security official has developed a log-in monitoring criteria that focuses on a) log-in attempts by terminated employees or business associates, b) log -in attempts that failed due to incorrect ID or password, c) log-in

attempts after non business hours by persons other than the physician on call.

6. The security official has developed a reporting list of the information to be reported for these log-in attempts.

7. The security official reviews these reports once a week. Discrepancies will be documented using the Security Incident Report form and this organizations reporting and response policies and procedures.

8. The security official periodically updates the log-in monitoring criteria, frequency of review, and related elements based on incidents and the results of our periodic technical and non-technical evaluation.

Security Incident Reporting and Response

Actions to Be Taken To Report and Respond To Security Incidents

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. THE DCO HAS REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS TO THE GUIDANCE PROVIDED BY OUR PROFESSIONAL LIABILITY INSURANCE CARRIER OR INFORMATION SYSTEMS VENDOR. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT DCO BEFORE CONTINUING.

2. The security official has met with the CMO and other management to ensure their awareness and adherence to these procedures.

3. The security official trained staff in these procedures and maintains staff training.

4. The security official has evaluated typical threats and probability of threats and trained staff to be aware of these.

5. The security official has reviewed the governing identity theft and any breach of unencrypted computerized personal information and or medical information, including health insurance information. The security official has evaluated the typical breaches that might occur where ePHI that

contains information that could be used for identity theft might be accessed in an unencrypted form by unauthorized persons. The security official has trained staff to recognize these incidents (such as theft of computers, unauthorized copying or backing up of data, outside “hacking” of systems, and so forth).

6. The security official has customized the Security Incident Form and distributed copies to all staff as well as instructed staff and management on how to complete the form.

7. The security official has trained staff and management to report both suspicious as well as actual incidents.

8. The security official has trained staff and periodically reminds staff to report physical security breaches as well as technical security breaches.

9. The security official will review any incident report the same day of receipt. In the event of a violation that does not have an incident report; the security official will review the violation on the same day and also document this using the incident report.

10. The security official will determine if the incident is an actual violation or just suspicious activity. If needed the security official will contact the systems vendor for assistance.

11. The security official will address actual violations immediately based on the nature of the violation. This may include activating the contingency planning procedure in this manual, the sanctions procedures or other relevant procedures.

12. In the event of a malicious action by a present or former employee or an outside individual the security official will immediately meet with the CMO, and together they will seek their attorney’s advice for further actions. They will also contact the professional liability carrier and if applicable the employee practice’s carrier.

13. If a security incident occurs where ePHI has been breached, the security official will investigate the breach immediately, and take all reasonable steps to determine the scope of the breach and restore the reasonable integrity of the data system. The security official will contact the practice’s attorney, or outside advisors to determine the most appropriate compliance plan, which will generally include notification of all affected patients.

14. If the security official or outside consultants determine that ePHI, medical information, personal information or health insurance information (as

defined in SB1386 and AB1298) in **an unencrypted form likely** was accessed by an unauthorized person or otherwise breached, the security official will *immediately* notify law enforcement; and, unless opposed by law enforcement, will notify all patients or individuals who had information on the ePHI file/program that was breached, consistent with the requirements of SB1386 and AB1298.

15. The security official will update all procedures to ensure that security measures are enhanced to minimize the likelihood of future violation. The nature of the update will depend on the seriousness and extent of the problem.

16. The security official will ensure that all data has been restored and integrity checked if applicable (for example in the case of infection by a virus).

Contingency Planning

Actions to Be Taken for Scheduled Backups and Criticality analysis

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. THE DCO HAS REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS. TO THE GUIDANCE PROVIDED BY OUR SOFTWARE VENDOR IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT THE DCO BEFORE CONTINUING.

2. The security official has reviewed the risk analysis and inventory of ePHI and applications as well as the criticality analysis.

3. The security official has determined those applications and the ePHI that are considered critical and part of this contingency plan. All subsequent procedures for back up recovery and restore will include these.

4. The security official will routinely update the contingency plan whenever a new application or form of ePHI is put into operation and deemed critical.

5. At the end of each day, SCNM runs an incremental back up. This archives the a) billing data, b) appointment scheduling data, c) word documents and d) accounting data files. (**Note**: If you use a critical application like an electronic health record, work with the vendor to establish the most appropriate back up process. This may require "mirroring" so each transaction is copied to a backup drive in real time, as well as incremental back up to removable disks.)

6. A daily hard copy report is run each day of the next week's appointments (along with contact information for each patient) and taken off site with the backup.

7. A full back up is run each Friday of the entire system, or as determined by the IT Department. This back up archives all data and applications on the system.

8. A set of back-ups will be kept for each incremental back up.

9. Each record will have that day's date written on a label attached to the tape after the backup is complete.

10. SCNM will house backups off site.

11. SCNM will house the weekly backups offsite and in a secure location.

12. The security official will ensure the backup is run as soon as practicable that day or the next day. The security official is responsible for ensuring an alternate staff person runs the back up in the case of the billing manager's absence.

13. Every month, SCNM will rotate the backup tapes so that the weekly tapes are used for incremental back up. This will be done starting with the oldest back up tape.

14. SCNM reviews the system back up logs each week to ensure the backup is operating. SCNM reviews each weekly full system back up tape to ensure its contents are complete.

15. SCNM will replace back up media every six months (or sooner based on manufacturer's advice).

16. SCNM will update the backup procedure to include new applications or data on both the incremental and weekly back up.

17. SCNM will review the backup procedure with new users and ensure their data is stored on the server and included in the back up routine.

18. SCNM will ensure that new applications and hardware are appropriately mapped to the backup procedure.

Actions to Be Taken For Disaster Recovery and Emergency Mode Operations

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. THE DCO HAS REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS TO THE GUIDANCE PROVIDED BY OUR SOFTWARE VENDOR [or other appropriate expert if applicable]. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT THE DCO BEFORE CONTINUING.

2. SCNM will maintain a printed list of all individuals who are involved in data backup and restore processes and emergency mode processes. This list will be kept up to date and copies given routinely to the DCO & CMO, and the applicable staff who will be instructed to keep this print out always available.

3. In the event of a disaster or other situation requiring restoring data, SCNM will begin by assessing the circumstance. The assessment will determine if the situation is: a) a computer or information system failure that is temporary, b) a computer or information system failure that will require an emergency mode operation, c) a hazard or event that is temporary or b) a hazard or event that will require an emergency mode operation.

4. SCNM will immediately locate the most current version of the data backup.

5. If the system and office will be accessible within 24 hours, SCNM will ensure that the backup is restored and that the data on the system is current.

6. If the system or the office will not be accessible within 24 hours, SCNM will arrange for access to the offsite storage location of the backups and restore the full system back up and then the most current incremental back up.

7. The security official will determine if any additional recovery is needed—if the system failure or hazard occurred during business hours and before the daily back up was completed, and if the system did not maintain files that are up to date, the security official will ensure that the missing data is re-entered into the system.

8. The security official will contact patients as applicable using the hard copy scheduling print out.

9. Once every month, the security official will test the restore process by restoring the most current incremental back up data. On a semi-annual

basis, the security official will restore the full system backup on the “hot site" system at the physician’s home. If the restore process does not work, the security official will correct any problem and ensure that it is working.

10. On an annual basis, the security official will test the disaster recovery and emergency mode operations plan in addition to the restore activity above. Failures in communication or related will be repaired. This test may be combined with this facility’s emergency preparedness plan testing.

11. If the recovery is a result of malicious software such as a virus or worm the security official will determine if quarantine of files is sufficient or if an entire system recovery and restore is needed. The security official will contact the vendors of the damaged applications data for their assistance.

Periodic Technical and Non-technical Evaluation Procedure

Actions to Be Taken To Develop and Maintain Periodic Technical and Non-technical Evaluation

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. THE DCO HAS REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS TO THE GUIDANCE PROVIDED BY OUR PROFESSIONAL LIABILITY INSURANCE CARRIER OR INFORMATION SYSTEMS VENDOR. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT THE DCO BEFORE CONTINUING.

2. The security official has met with the CMO and other management to ensure their awareness and adherence to these procedures.

3. The security official has reviewed the risk analysis and determined this organization’s areas of vulnerability, current measures, and new measures in place to reduce vulnerabilities and threats associated with safeguarding ePHI and maintaining its availability.

4. The security official has met with the network vendor and our practice management and electronic medical records vendor [Insert additional as appropriate] to determine the best way to periodically evaluate our technical measures and safeguards.

5. The security official will follow all other procedures in place for auditing suspicious activity, integrity and access, physical security management, malicious software detection, security incident reporting and so forth.

6. The security official, every six months will review and re-conduct the risk analysis to evaluate changes that could weaken the security measures in place.

7. The security official will also evaluate physical environment changes and technical changes.

8. The security official will document the results of the evaluation and ensure appropriate changes and modifications are made to security measures and systems.

Physical safeguards

Actions to Be Taken for Physical safeguards and access controls

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. THE DCO HAS REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS TO ANY GUIDANCE PROVIDED BY OUR PROFESSIONAL LIABILITY INSURANCE CARRIER. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT DCO BEFORE CONTINUING.

2. The security official has reviewed this procedure the CMO.

3. The security official has completed a detailed inventory of the electronic information systems in this organization, and their location. The security official has also included this in this organization's risk analysis and identified all vulnerabilities.

4. The security official will keep this inventory up to date and modified if there is a change to the physical site.

5. The security official has determined a contingency plan for access to the facility to retrieve backup data and other key information needed for emergency operations, if at all possible, in the case of a disaster, to retrieve back up data and other key information needed for emergency operations. This plan is described in the Disaster recovery and emergency mode operations procedure.

6. Door locks and alarms are kept in working order.

7. The security official maintains a detailed log of all individuals with keys and alarm codes.

8. The security official has ensured that adequate fire protection exists for this facility.

9. Based on the risk analysis, the security official has determined and implemented appropriate power conditioning and uninterruptible power supply for servers and key workstations. The batteries and related components of these systems will be kept in working condition and periodically tested.

10. The computer server, located in the billing office, will be kept secure via a secondary lock on the billing department door.

11. Laptops, Personal Digital Assistants (PDAs) or other mobile devices (including flash data drives) that contain or transmit ePHI in [offices] are kept locked with a desk lock cable, or otherwise kept secure from theft.

12. Laptops, Personal Digital Assistants (PDAs) or other mobile devices that contain or transmit ePHI (including flash data drives, zip disks, CDs etc) that are removed from the office and used remotely, are kept secure during travel and transit and not left unattended.

13. Laptops, Personal Digital Assistants (PDAs) (including flash drives, zip disks, CDs etc) or other mobile devices that contain or transmit ePHI that are used at the residence of the authorized employee, are kept secure and protected from unauthorized use by family or friends.

14. All visitors must sign-in and establish their identity before access to any part of this office where electronic PHI is stored.

15. All software and hardware vendors will be signed in and supervised while they access the information systems.

16. All repair personnel, including those provided by the building management, who repair or maintain doors, locks, walls, windows or other physical structures that could be compromised will be supervised and the integrity of the structure and related security checked after completion of repairs.

17. Alarm codes are changed whenever an employee is terminated, and routinely every 60 days.

18. Workstations and media immediately located near the workstation are kept secure from visitors and non-staff. Workstations will routinely be checked to ensure their location reduces visibility by non-staff.

19. When staff uses a hallway computer workstation, care is taken to stand in front of the screen and limit exposure to patients or visitors.

20. . Whenever hardware is relocated, and the hardware contains critical ePHI that is not already backed-up, an exact back up will be done of the ePHI on that hardware prior to moving or relocation. The security official will ensure the backup is accurate (as necessary by having vendor support) and will personally ensure the backup is available until the hardware is relocated and operational.

21. The security official maintains a current log of all hardware and its location; this log is updated whenever hardware is received, moved or discarded.

22. Whenever hardware is discarded, the security official will ensure that all data has been removed using a reformatting or similar option (such as a commercial software sanitizer) to clear the permanent memory and any RAM memory. [Alternatively consider using an option that "shreds" or otherwise certifies destruction of hardware. **Note:** some organizations are taking the position that they will not recycle old hardware or media with PHI nor donate it to other organizations because of the inherent risk that it will contain some ePHI that an expert could uncover. Instead, they use a secure destruction service. This also extends to hardware that is "swapped" for the purpose of repair.]

23. The security official will maintain a key to the CMO's home solely for the purpose of access during emergency mode operations. The security official will attempt to inform the physician before such emergency access and afterwards.

Technical safeguards

Actions to Be Taken for Technical Safeguards and Access Controls

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. THE DCO HAS REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS.

2. The security official has reviewed this procedure the CMO.

3. The SCNM has completed a detailed inventory of the electronic information systems and electronic PHI in this organization, and their location. The security official has also included this in this organization's risk analysis and identified all vulnerabilities.

4. SCNM will keep this inventory up to date and modified if there is a change to the hardware or software inventory, or methods of creating, storing or transmitting electronic PHI.

5. Based on the ePHI inventory and risk analysis, the SCNM will implement encryption of data at rest (on servers, workstations, backup devices and its media, or on portable devices) and of data being transmitted, if possible and practical to mitigate the risks to either ePHI, or personal data, medical information and health insurance information. In the event the security official cannot ensure encryption, the reasons for this decision and alternate safeguards in place will be documented.

6. As established in other procedures, the security official will always ensure that any individual or software (for example remote software that uploads your health care claims) always has a user level identification code as well as password level protection. The job responsibility with respect to PHI form will continually be updated to document this.

7. Where applicable the security official will ensure that perimeter access (firewalls) require authentication by user ID, MAC address, or IP address.

8. SCNM will maintain a secondary offsite list of all administrative privilege and access codes. This list as well as primary and secondary access methods will be part of the contingency plan.

9. SCNM will ensure that the automatic log off feature is always enabled for each workstation and user and periodically ensure that it has not been

disabled or the timeout feature modified (for example the time away before log off has been increased from 5 minutes to 5 hours!).

10. The SCNM will ensure that the encryption feature is activated on all system files maintained on the server.

11. The security official will determine whether or not the email this practice uses for appointment scheduling and correspondence contains PHI and, if so, if this PHI should be protected if so, the security official will ensure that the email this practice uses for appointment scheduling and correspondence uses encryption software. The security official will also determine if a digital certificate is needed for regular transmission of ePHI.

12. The security official will ensure that critical data files are kept in read only format wherever possible and that the fewest number of individuals possible have access to modify. The security official will implement integrity review controls working with the vendor to periodically review the integrity of the database and version numbers.

13. The security official will ensure that all data transmissions to the claims clearing house are done through a secure transmission protocol supplied by the clearing house. Staff will be trained to never transmit electronic PHI unless it is encrypted or sent through a secure transmission protocol.

14. The security official will ensure that the physicians and clinical staff do not communicate via email or the Internet with other health care providers unless the digital certificate or other accepted authentication feature is used.

15. The security official and Information Technology have ensured that any authorized person who chooses to remotely access ePHI will do so only with a secure system.

16. If wireless access points and systems are used within the facility, the security official will ensure that the wireless access requires encryption and sufficient authentication to prevent unauthorized access. The security official will ensure that the wireless encryption method used is strong and current enough to be reasonably resistant to exploitation. The security official will review the risk analysis and determine if devices that access the network through a wireless access point require additional authentication such as MAC address.

17. The security official will enable automatic and periodic scans using a) the antivirus and malicious code protection software and b) the spy-ware software. Scans will review all system files and programs. Infected files will be quarantined and/or rebuilt.

18. The security official will enable automatic and periodic scans of each user's workstation, including laptops used for remote access using a) the antivirus and malicious code protection software and b) the spy-ware software. Scans will review all system files and programs. Infected files will be quarantined and/or rebuilt.

19. The security official will review all applications in use; working with the vendors the security official will ensure the applications are maintained with appropriate patches and updates to mitigate known vulnerabilities.

20. The security official will supervise all technical repairs to the hardware or any software program; all technicians must sign in and be verified in identity. The security official will test the system for integrity after the repair has been completed.

21. The Security Official will ensure that all passwords are "strong," that is, they are at least (6)(8) characters in length and have a combination of letters, numbers and at least one symbol. Passwords are changed every [60][180] days. (Note: Best practices in security now advise use of pass phrases of 12 characters in length or more.)

22. The security official once every two weeks will review the audit logs set up by the network vendor of system activity to detect unauthorized access or suspicious activity; these logs will be reviewed weekly after the termination of staff for a period of one month.

23. The security official, where applicable, will ensure that all servers, workstations, and other devices are configured to prohibit any disabling of security controls like log offs, automatic updates, and so forth without Administrator or similar privilege level access.

Actions to Be Taken for Implementing Security Policies and Procedures

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. THE DCO HAS REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS. TO ANY GUIDANCE PROVIDED BY OUR PROFESSIONAL LIABILITY INSURANCE CARRIER. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT DCO BEFORE CONTINUING.

2. The security official has reviewed this procedure the CMO and other appropriate management.

3. The security official has completed all the steps in the Risk Analysis PrivaGuide.

4. The security official has reviewed the PrivaGuides that discuss implementing the security rule as well as completing a risk analysis.

5. The security official has identified all the changes in procedure and measures implemented to meet the required and addressable rules.

6. The security official, using this policy and procedure template, has modified this template to incorporate this organization's unique and specific security measures.

7. The security official periodically reviews and updates these policies and procedures.

8. The security official has ensured that this organization's leadership has adopted the security policies as a matter of corporate record.

LAB SAFETY PROCEDURES AND POLICIES

Medical Center Procedure:

Purpose of Procedure: To assist the minor surgical staff in decontaminating, cleaning, maintaining, handling, storing, and/or sterilizing surgical instruments.

Procedure Title: Cleaning and Caring for Surgical Instruments	**Procedure Number: 1024**
Department/Staff: Lab	
Effective Date of Procedure: 9/21/10 **Procedure Updates:** 12/10/12	
Procedure Approved by: Safety Committee	**Signatures:**
Policy Implemented by: Laboratory Manager	**Signatures:**

Definitions:

Decontamination: The process by which contaminants are removed, either by hand cleaning or mechanical means, using specific solutions capable of rendering blood and debris harmless and removing them from the surface of an object or instrument.

Procedure:

A. Surgical instruments and equipment need to be cleaned, handled, and used according to manufacturers recommendations.
B. Instruments should be kept free of gross soil during surgical procedures.
    1. Instruments need to be wiped with sponges moistened with sterile water when there is a chance that they will have gross soiling during a surgical procedure.
    2. Dry instruments thoroughly and then air dry 10 minutes before packaging. Corrosion, rusting, and pitting occur when blood and debris are allowed to dry on surgical instruments.
C. Effective and timely decontamination of instruments will be performed.
    1. All instruments opened on the sterile field require decontamination.
    2. Staff performing decontamination should where personal protective equipment that includes an impervious gown, clean gloves, and a mask. A face shield is also recommended if splashing is likely to occur.
    3. Instruments need to be taken apart so that all surfaces are exposed.
    4. All instruments with the exception of power instruments will be submerged in warm water with instrument cleaning germicide.
    5. Instruments will be cleaned and rinsed while completely submerged in water. This will help prevent aerosolization.
    6. If grossly soiled, use a brush to clean.
    7. Rinse under warm running water.
D. Instruments need to be inspected and prepared for sterilization after decontamination.
    1. Instruments need to be inspected for:
        a. cleanliness

    b. proper functioning and alignment
    c. corrosion, pitting, burrs, nicks, and cracks
    d. sharpness of cutting edges
    e. loose set pins
    f. any other defects.
2. Instruments in disrepair will be labeled and taken out of service until properly replaced or repaired.
3. Instruments need to be dried thoroughly after decontamination.
4. Instruments with removable parts will be reassembled before packaging for sterilization.

Medical Center Procedures:

Purpose of Procedure: To be in compliance with the state reporting requirements.

Procedure Title: Reporting of Communicable Diseases	**Procedure Number: 1014**
Department/Staff: Lab	
Effective Date of Procedure: **Procedure Updates:** 2/18/15	
Procedure Approved by:	**Signatures:**
Procedure Implemented by:	**Signatures:**

Reporting of suspected or confirmed communicable disease is mandated under the Arizona Administrative codes.

Procedure:

1. Disease reports are to be submitted within five (5) working days of diagnosis, treatment or detection. However, some conditions must be reported within 24 hours or only during outbreaks.

2. Complete reporting specifications and timelines can be found at:
   http://www.azdhs.gov/phs/oids/pdf/rptlist.pdf

3. Communicable disease reporting forms are available at:
   http://www.azdhs.gov/phs/oids/pdf/forms/cdr_form.pdf

4. Completed forms are to be mailed or faxed.

   Mailing address:

   Maricopa County Department of Public Health
   4041N.Central Ave
   Phoenix, AZ 85012

   Fax and phone numbers:

   HIV/AIDS: F: 602-372-6035; P: 602-506-2934

   STDs: F: 602-506-6916; P: 602-506-1678

   TB: Must be phoned in: 602-506-8282

   Animal bites: Must be phoned in: 602-506-7387

   All Others: F; 602-372-8935; P: 602-506-676

Medical Center Procedure:

Purpose of Procedure: Provide staff with direction for achieving high level disinfection of instrumentation and durable equipment

Procedure Title: High Level Disinfection	**Procedure Number: 1023**
Department/Staff: Lab	
Effective Date of Procedure: 9/21/10 **Procedure Updates:**	
Procedure Approved by: Director Of Clinical Operations	**Signatures:**
Procedure Implemented by: Laboratory Manager	**Signatures:**

Procedure:

A. Items that come in contact with nonintact skin or mucous membranes are considered semi critical and should receive a minimum of high level disinfection immediately before use.
B. Items need to be thoroughly cleaned and decontaminated before disinfection.
    1. Meticulous physical cleaning must precede disinfection procedures.
    2. Instruments must be rinsed and dried before being subjected to the disinfection process.
C. High Level Disinfection
    1. Items to be chemically disinfected should be completely immersed in the disinfectant solution.
       High Level Disinfection can be achieved after 20 minutes of immersion as long as the solution is 2% gluteraldehyde. The item should be rinsed with sterile water and presented to the sterile field immediately after rinsing.
    2. Keep the high level disinfection in a covered container and used in a ventilated area
    3. Staff using the high level disinfectant should be wearing eyewear such as facial shields, gloves, masks, and moisture repellent jumpsuits or aprons

Medical Center Policy and Procedure:

Purpose of Policy: To ensure that potential hazards and hazard control measures for chemicals used are understood by staff.

Policy Title: HAZARDOUS CHEMICALS	**Policy Number: 1005**
Department/Staff: Lab	
Effective Date of Policy: 10/20/2005 **Policy Updates:** 8/30/2008	
Policy Approved by: Director of Clinical Operations	**Signatures:**
Policy Implemented by: Laboratory Manager	**Signatures:**

Procedure:

1) MSDS Manual is located on shelf in Laboratory.
2) Refer to the MSDS Manual for identification and location of hazardous chemicals used by SNMC facilities.

Procedure Implementation Date:____
Procedure Communications: _____

Medical Center Procedure:

Purpose of Procedure: To reduce the risk of injury to laboratory employees

Procedure Title: LAB SAFETY	**Procedure Number: 1008**
Department/Staff: Lab	
Effective Date of Procedure: 12/13/2005 **Procedure Updates:** 8/30/2010	
Procedure Approved by: Director of Clinical Operations	**Signatures:**
Procedure Implemented by: Laboratory Manager	**Signatures:**

Procedure:

1) **All employees are required to become familiar with and/or receive training in the following:**
   a) Lab policies and procedures-Upon hiring, then annually.
   b) Blood Borne Pathogen (OSHA)/HIPAA training-Upon hiring, then annually.
   c) Fire Safety/ Emergency Action Plan-Upon hiring, then annually.
   d) Hazard Communication-Upon hiring then annually.
   e) Exposure Control Plan-Upon hiring.

2) **Fire Extinguishers:**
   a) There is a fire extinguisher in the lab mounted on the wall in the back hallway.
   b) To use fire extinguisher, locate the small lever on top sealed with plastic. Pull the pin. Aim hose or nozzle at the base of the fire. Squeeze the double handle to produce the extinguisher powder.

3) **Maintenance of Fire Extinguishers:**
   a) Fire extinguishers will be visually inspected by facility employees monthly and annually checked by Aidant Fire Protection (480-607-4600).
   b) This will be documented on the maintenance log located on the lab refrigerator.
   c) There is an annual Fire Inspection by the Tempe Fire Department. This will be documented on the lab maintenance log.

4) **Eyewash Station:** (attached to the sink faucet in laboratory)
   a) Turn on the cold water side of the faucet. Pull the silver button to activate the eye wash. Green caps will pop off. Flush foreign objects or chemicals from the eye with copious amounts of water (15 minute wash). Turn off the water when flushing is complete and replace the green protective caps.

   Maintenance of Eyewash:
   b) Lab employees are responsible for weekly inspection and testing of eyewash station by following the above procedure. This will be documented on the maintenance log located on the lab refrigerator.

Medical Center Procedure:

Purpose of Procedure: To assure proper packaging for instruments.

Procedure Title: Packaging surgical instruments for sterilization	**Procedure Number: 1021**
Department/Staff: Lab	
Effective Date of Procedure: 9/21/10 **Procedure Updates:**	
Procedure Approved by: Director Of Clinical Operations	**Signatures:**
Procedure Implemented by: Laboratory Manager	**Signatures:**

Procedure:

A. Peel Packages
   1. Peel packages need to have as much air removed as possible before sealing. Air acts as a barrier to heat and moisture. Expansion of air my cause rupturing of packages during the sterilization process.
   2. Peel packages that have a break in the seal once the item is sterilized needs to be considered contaminated.
   3. Peel packages will be hermetically sealed. Pressure is applied to the mating surfaces of the self sealing pouches. During sterilization, the seal adhesive cures to become a permanent seal.
   4. Packages will be inspected for intact seals before and after sterilization and again before use.
   5. Double peel packaging is not routinely required however if multiple small items are packed in the same pouch, it will facilitate aseptic presentation to the sterile field
   6. If double peel pouch packaging is used, it will be used in a manner as to avoid folding the inner package to fit into the outer package.
   7. Peel packages need to open without tearing, linting, shredding, or delaminating. The sterilized items in such peel pouches should be considered contaminated.

B. Wrapping
   1. Package contents need to be assembled, handled, and wrapped in a manner that provides for an aseptic presentation of package contents.
   2. The appropriate size wrapping material should be selected to achieve adequate coverage of the item being packages.
   3. Wrap the item securely to prevent gapping, billowing, and air pockets from forming, which could compromise sterility.
   4. Sequential wrapping using two barrier free wrappers provides a tortuous pathway to impede microbial migration and permits ease of presentation to the sterile field.

C. Labeling
    1. Packages to be sterilized should be labeled. The label information needs to include:
        a. A description of package contents
        b. Initials of the packages assembler
        c. The load number and date
    2. Label information should be documented on pressure-sensitive tape and not on the packaging material.
    3. Peel packages may be labeled on the plastic portion or on the self sealing tab. Markers used to label packaging systems need to be indelible, nonbleeding and nontoxic. Felt tip ink pens or a very soft lead pencil may be used.

D. Event related sterility-an event must occur to compromise package content sterility. In other words once a package is processed through the sterilizer, it is considered sterile until:
    1. Multiple handling leads to seal breakage or loss of package integrity.
    2. Moisture penetration
    3. Airborne contamination.

Medical Center Procedure:

Purpose of Procedure: To improve overall laboratory operations

Procedure Title: QUALITY CONTROL (QC) GUIDELINES	**Procedure Number: 1012**
Department/Staff: Lab	
Effective Date of Procedure: 10/05/2005 **Procedure Updates:** 8/4/2010	
Procedure Approved by:	**Signatures:**
Procedure Implemented by: Laboratory Manager	**Signatures:**

Procedure:

Quality control is a process in which procedures are performed to ensure that the test results being reported are accurate and reliable.

1) QC will be performed and recorded every day of testing or per specifications for the instrument or method.
2) Quality Control specimens will be run in the same manner as patient specimens.
3) Quality Control results are recorded in the Fflexesuite LIS.
4) QC records will be maintained for a period of at least 2 years.

If Quality Control Results Fall Outside of Specified Ranges

1) Testing personnel will review quality control results. Specific ranges are set for each control reagent and can be found on the package insert. If testing falls outside of these ranges, then corrective action must be taken and noted in Fflexesuite before patient specimens are tested that day.
2) No results are reported out until QC is run and accepted.
3) The Urisys weekly calibration strip is to be taped into log in QC manual and initialed by lab tech performing the calibration.
4) Each month, QC data will be reviewed by the Lab Manager or staff appointed by the Lab Manager for shifts and trends. This will be recorded and be available for future reference.
5) The Lab Manager will periodically review QC data with laboratory personnel.

Preventative Maintenance

1) To ensure that test results are valid, daily temperature and humidity checks must be performed on all equipment or environments that are temperature dependent.
2) All temperatures and humidity checks must fall within the established ranges before a specimen can either be reported or stored.

Medical Center Procedure:

Purpose of Procedure: 1) To document failures of FDA approved devices to ensure that there is appropriate follow-up.
2) To file the appropriate forms with the FDA regarding failure of FDA approved devices that result or have the potential to result in harm to a patient or employee.

Procedure Title DOCUMENTING AND REPORTING FAILURES OF FDA APPROVED DEVICES	**Procedure Number: 1013**
Department/Staff: Lab	
Effective Date of Procedure: 04/30/2008 **Procedure Updates:** 8/30/2008	
Procedure Approved by: Director of Clinical Affairs	**Signatures:**
Procedure Implemented by: Laboratory Manager	**Signatures:**

Procedure:

1) Employees must notify the lab supervisor/manager of any failure of a FDA approved device that result in or have the potential to result in harm to a patient or employee. The lab supervisor/manager is responsible for reviewing documented problems with devices, and contacting the FDA in the event of any adverse events.
   a) Report adverse events, product problems or product use errors.
   b) Report product problems –quality, performance or safety concerns.
   c) Report serious adverse events.
2) Methods of reporting
   a) Fill in the sections that apply to your report
   b) Use a separate form for each patient
   c) Report either to FDA or manufacturer (or both)
      i) Fax report to 1-800-FDA-0178 (1-800-332-0178); or
      ii) Phone report to 1-800-FDA-1088 (1-800-332-1088); or
      iii) Report online at www.fda.gov/medwatch/report.htm
   d) Keep a copy of report on file.

Medical Center Procedure:

Purpose of Procedure: To provide instructions for proper sterilization of surgical instruments

Procedure Title: Sterilization of Surgical Instruments	**Procedure Number: 1022**
Department/Staff: Lab/Medical Assistant	
Effective Date of Procedure: 9/21/10 **Procedure Updates:** 1/14/15	
Procedure Approved by: Director Of Clinical Operations	**Signatures:**
Procedure Implemented by: Laboratory Manager	**Signatures:**

Procedure:

A. All items to be sterilized are packaged according to Procedure.
B. Using the sterilizer
    1. Select and press the pouches button then press start.
    2. Pouches will sterilize for five minutes and then dry for 30 minutes. Do not open the sterilizer while the items are drying because it could cause water to settle onto the packaging thereby contaminating it.
    3. Programmed 1 button is for Dr. Marchese's pessaries only.
    4. Trays must be used at all times when operating the sterilizer.
C. Sterilizer efficacy testing (Spore testing)
    1. Spore testing should be conducted after 5 cycles.
    2. We have purchased spore testing kits from Enviro-Tech.
    3. Follow directions for spore testing using test strips.
    4. Place tested strip into pre-paid envelope and mail to Enviro-Tech.
    5. Environ-tech will transmit results via email to the Laboratory Manager.
    6. All spore testing should be recorded in the spore testing log.
    7. Positive biological indicator test results need to reported to the Director of Clinical Operations immediately so appropriate action can be taken.
D. Recording in the sterilizer log:
    1. Cycle used (pouches or packs)
    2. Load number and date
    3. Load contents
    4. Exposure time and temperature
    5. Operator's name
E. A sterilization process indicator needs to be used in each package to be sterilized.
F. Maintenance records for sterilizer need to include:
    1. Date of service
    2. Sterilizer model and serial number
    3. Description of malfunctions (if any)
    4. Name of person performing maintenance

5. Results of biological validation testing
6. Name of person requesting the service
7. Signature and title of person acknowledging completed work.

Medical Center Procedure:

Purpose of Procedure: To protect the employee/student from becoming infected or infecting others

Procedure Title: Violation of safety standards protocols	**Procedure Number: 1017**
Department/Staff: Lab	
Effective Date of Procedure: 10/20/2005 **Procedure Updates:** 8/30/2008	
Procedure Approved by: Director of Clinical Operations	**Signatures:**
Procedure Implemented by: Laboratory Manager	**Signatures:**

Procedure:

1) First Violation
   a) The employee will be verbally counseled and will be required to read the Universal Precautions, Standard Precautions and/or Transmission-Based Precautions Guidelines.
   b) The manager/supervisor will document that a verbal discussion took place and describe the content of that discussion.
2) Second Violation
   a) The employee will be given a written reprimand, documenting the second incident and the previous verbal discussion.
   b) The employee will be required to attend a mandatory in-service of Universal Precautions on a given date and time.
3) Third Violation
   a) The employee will be given a written probation form documenting the third incident.
4) Fourth Violation
   a) Employee will be discharged from employment. The fourth incident and subsequent termination will be documented on the employee's record and discharge form.

PRACTICE STANDARDS SAFETY PROCEDURES AND POLICIES

SCNM Medical Center Procedure:

Purpose of Procedure: To ensure all acupuncture needles in exam rooms are accounted for.

Procedure Title: Acupuncture Needle Safety	**Procedure Number: 0056**
Department/Staff: Medical Center Employees, Physicians and Students	
Effective Date of Procedure: 9/10/10 **Procedure Updates:** 4/27/11, 5/25/11, 2/11/15	
Procedure Approved by: Executive Vice President	**Signatures:**
Procedure Implemented by:	**Signatures:**

Procedure:

1. Each acupuncture needle must be counted when placed into patient and documented in patient's medical record.
2. The mobile sharps container must be taken to bedside when removing needles from patient.
3. Each acupuncture needle must be counted when removed from patient and documented in patient's medical record.
4. Patient may not be released until all needles are accounted for and disposed of in the sharps container.
5. Rooms will be swept with magnetic sweeper for needles after each acupuncture patient and at end of each rotation that acupuncture was performed.
6. Sweeper will be visually inspected for any needles after completing sweep.
7. If acupuncture needles are located on sweeper, individual will place on gloves and a forceps will be used to remove needle and place into sharps container.
8. If all needles are not accounted for after removal and sweeping, recheck patient and linens.
9. If after recheck needles are not account for an incident, report will be generated.

SCNM Medical Center Procedure:

Purpose of Procedure: Use of the Automatic External Defibrillator

Procedure Title: Use of the AED	**Procedure Number: 0023**
Department/Staff: Medical Center Employees	
Effective Date of Procedure: **Procedure Updates:** 8/10/11, 5/15/12	
Procedure Approved by: Executive Vice President	**Signatures:**
Procedure Implemented by:	**Signatures:**

Procedure:

1. Establish loss of consciousness and call for help.
2. Establish absence of respirations and circulation.
3. Indicate a specific individual to call 911.
4. Indicate a specific individual to locate the AED in the Emergency Crash Cart.
5. A designee needs to record onset of arrest, time and number of AED shocks, medications given, procedures performed, cardiac rhythm, use of CPR, and client's response (the form will be found in the Emergency Crash Cart).
6. Start chest compressions until AED arrives.
7. Place the AED next to the client's chest or head.
8. Turn power on by pushing the "On/Off" button and then follow the instructions the AED will indicate.
9. Observe the status indicator and the battery icon on the screen.
    a. The status indicator will provide a warning when the battery is low, depleted, or not in place.
    b. The battery icon indicates the battery level.
10. Stop CPR and place the AED pads as indicate by the AED
    a. Remove all clothing covering chest.
    b. Wipe all moisture away from chest.
    c. Remove excess hair from chest if necessary.
    d. Peel off the backing from electrode pads.
    e. Place pads on patient as indicated above.
    f. Verify that the pads connector is plugged into the AED.
11. Clear rescuers away from victim as the area needs to clear for the AED to analyze the rhythm accurately.
12. Allow AED to analyze rhythm.
13. Announce loudly before shocks to clear area near the victim.
14. Shock(s) are delivered as indicated by AED. Inspect pad adhesion to chest wall between series of shocks.
15. Check for signs of circulation between shocks as directed by the AED.

Medical Center Procedure:

Purpose of Procedure: To prevent transfer of infection of HIV, Hep-B, or other infectious diseases

Procedure: Reporting Possible Blood-Borne Pathogen Exposure	**Policy Number:**
Department/Staff: SCNM	
Effective Date of Policy: **Policy Updates: 11/13/14**	
Policy Approved by: Medical Center Steering Committee	**Signatures:**
Policy Implemented by:	**Signatures:**

Procedure:

1. The exposed individual notifies their supervising physician or supervisor of possible exposure.
2. The Possible Blood-Borne Pathogen Exposure Report will be initiated by the supervising physician or supervisor.
3. The exposed individual or supervising physician needs to call Banner Occupational Health Services at 602-747-8364
4. The supervising physician or laboratory staff will inform the source patient of the incident and obtain consent for HIV, HEP-C, and HBV testing. The source patient will be drawn at SCNM Medical Center prior to leaving facility when possible.
5. If the source patient refuses, or the test is positive for HIV, the exposed individual shall be placed on HIV protocol further evaluation will occur through Banner Health
6. If the exposed individual is an employee then they are required to submit Form to ADOSH. The form is available on the website:
   http://www.ica.state.az.us/Claims/Forms/Claims_WorkersReportOfInjury.pdf
7. If the exposed individual is an employee then the employer is required to submit form to ADOSH. The form is available on the website:
   http://www.ica.state.az.us/Claims/Forms/Claims_EmployerReportOfInjury.pdf
8. The Possible Blood-Borne Pathogen Exposure Report when completed is directed to the Safety Officer.

SCNM SOUTHWEST COLLEGE OF NATUROPATHIC MEDICINE & HEALTH SCIENCES
MEDICAL CENTER

POSSIBLE BLOOD-BORNE PATHOGEN EXPOSURE REPORT

This form should be filled in by the exposed individual or Supervising Physician involved **immediately** following a possible blood-borne pathogen exposure. It should be forwarded **by end of the day** to the Safety Officer responsible for SCNM Medical Center. *Please print all information.*
***In the case of an Injury (including needle stick), employees are required to submit the form at the indicated website to ADOSH:**
http://www.ica.state.az.us/Claims/Forms/Claims_WorkersReportOfInjury.pdf

❑602-747-8364 Called
❑Source Individual Drawn
❑Post Exposure Report completed
❑Submitted to:_____
Date/Time_____

Exposed Person Involved		
Name:	Date of Birth:	Phone (H):
Home Address:		
Status: ❑Student ❑Physician ❑Employee ❑Patient/Visitor ❑Other Provider: _____		
Location: ❑College ❑SNMC ❑Extended site: _____ ❑Offsite: _____		
Called 602-747-8364 within 15 minutes of possible exposure identifying self from Southwest College of Naturopathic Medicine❑		

Details of Incident		
Date of incident:	Time of incident: am/pm	Location:
Explain the incident and the circumstances prior to the incident? (Including equipment or material used.)		
Nature of Injury: ❑Needle Stick ❑Bruising ❑Chemical exposure ❑Stress/Anxiety ❑Body fluid exposure ❑Puncture ❑Pain/Discomfort only ❑Other *(please specify)*: _____		

Source Individual	
Name:	Phone:
Home Address:	
Status: ❑Student ❑Physician ❑Employee ❑Patient/Visitor ❑Other Provider: _____	
❑Yes ❑No Source patient has consented to have his/her blood tested for HBV, HCV, HIV. ❑Yes ❑No Legally required consent cannot be obtained. Reason _____ ❑Yes ❑No Source patient is known to be infected with HBV, HCV, HIV. If yes, specify_____ ❑Yes ❑No Results of source patient's tests have been made available to the exposed employee.	

Identify Sharp Involved
Type _____ Brand _____ Model _____ Did the device being used have engineered sharps injury protection? ❑Yes ❑No ❑Don't Know Was the protective mechanism activated? ❑Yes-Fully ❑Yes-Partially ❑No Did the exposure incident occur: ❑Before ❑During ❑After Activation
Exposed Individual: If sharp had no engineered sharps injury protection, do you have an opinion that such a mechanism could have prevented the injury? ❑ Yes ❑ No Explain _____ Do you have an opinion that any other engineering, administrative or work practice control could have prevented the injury? ❑Yes ❑No Explain _____

(This Area To Be Filled Out By Attending Physician)
Called 602-747-8364 within 15 minutes of possible exposure identifying self from Southwest College of Naturopathic Medicine ❑
Did this task require Personal Protective Equipment (PPE)? ❑Yes ❑No
Was correct PPE being used at the time of incident? ❑Yes ❑No
PPE worn: ❑Eye Protection ❑Gloves ❑Gowns ❑Face Protection ❑Footwear ❑Hearing Protection
Attending/Supervising Physician: Date:

SCNM Medical Center Procedure:

Purpose of Procedure: Changing Intravenous Solutions

Procedure Title: Changing Intravenous Solutions	**Procedure Number: 0024**
Department/Staff: Clinical Physicians/Clinical Students	
Effective Date of Procedure: **Procedure Updates:** 2/11/15	
Procedure Approved by: Executive Vice President	**Signatures:**
Procedure Implemented by:	**Signatures:**

Procedure:

1. Verify the physician's order.
2. Determine patency of IV site.
3. Determine the compatibility of all the IV fluids and additives with the current solution and solution to be hung.
4. Prepare to change the solution when less than 25-50 ml fluid remains in the infusing bottle or bag.
5. Explain the procedure to the client.
6. Maintain drip chamber half full.
7. Perform hand hygiene and apply clean gloves.
8. Prepare new solution for changing.
    a. Verifying the solution and additives with the original order with a correct label.
    b. Ensure the solution is not cloudy and no precipitation or no sediment noted is noted.
9. Adjust roller clamp to reduce flow rate.
10. Remove old solution from IV pole.
11. Remove spike from old solution and correctly insert spike into new solution while maintaining a sterile technique.
12. Hang new bag or bottle of solution on the IV pole.
13. Check for air in IV tubing. If air is present, adjust the roller clap to the "off" position and perform the air removal technique listed below.
14. Ensure that the drip chamber is half full.
15. Regulate the flow rate to the prescribed rate.
16. Assess client to determine response to IV fluid therapy.
17. Identify unexpected outcomes. See separate IV manual.
18. Record amount and type of fluid infused.
19. Record the assessment of the insertion site.

Air Removal Technique

1. Obtain 10cc syringe and an alcohol pad.
2. Swab the injection port with alcohol.
3. Attach the 10cc syringe to the injection port.
4. Kink the tubing below the injection port to ensure the air does not flow into the patient. The tubing is to remain kinked while withdrawing the air.
5. Open the roller clamp and withdraw the air from the tube by pulling back on the plunger of the syringe.
6. Remove the 10cc syringe.
7. Adjust the roller clamp to the prescribed flow rate.

SCNM Medical Center Procedure:

Purpose of Procedure: Ensure safety of patient as well as proper colonic therapy treatment.

Procedure Title: Colonic Procedure	**Procedure Number: 0005**
Department/Staff: Medical Center Employees	
Effective Date of Procedure: **Procedure Updates:** 1/14/15	
Procedure Approved by: Executive Vice President	**Signatures:**
Procedure Implemented by:	**Signatures:**

Procedure:

1. Turn on green button on colonic machine marked "power"
2. Turn on UV light on filter system (black toggle switch on left side of filter hood
3. Turn on water supply – under filter system there are a pair of red and blue handles. Parallel – is "on" and Perpendicular is "off"
4. Preheat water by attaching nylon reinforced hose from water inflow to water/waste outflow until water reaches desired temp. (95-100 degrees) Set water temp. using master valve; the red button on the master valve allows you set temp. above 100 degrees. Drain warm-up hose; hook on right side of machine.
5. Set up the colonic table (supplies in cabinet over sink)
    a. Place two under pads on table lengthwise
    b. Place paper towel on pillow
    c. Set out unopened disposable pack
    d. Set out fresh folded gown on table
6. Patient set-up for colonic:
    a. Show new patient the sterile disposable pack. Explain water inflow and water/waste outflow, speculum and sterile lubricant
    b. Show new patient colonic machine. Explain the basic process of disinfecting machine between appointments
    c. Request that patient put on gown with opening in back, taking off closing below the waist. Request patient urinate before treatment.
    d. While patient is changing in the bathroom set-up colonic pack:
        i. Put on gloves, fold paper towel for use with gel and speculum
        ii. Cut open pack, empty and place plastic bag on stool; set paper towel with speculum and gel on it
        iii. Attach water inflow hose, hook into handle
        iv. Lubricate water/waste outflow hose at both ends with sterile gel (hose will leak without gel); hook hose onto handle
        v. Attach water inflow hose to pseculum

e. Have patient sit on table; then roll onto left side, facing the wall, with knees bent and head supported by pillow
f. Lubricate speculum with gel. Present speculum with inflow hose at 90 degree angle to table. Gently insert keeping steady pressure on speculum and turning speculum 90 degrees to the right until it is inserted (water inflow hose must be perpendicular to the table with patient on back). Have patient roll onto their back while holding speculum in place. Make sure inflow hose is not bent over or under patient's leg. Slowly turn on flow control with waste control set to empty to flush air from the hoses.
g. Administering colonic to patient:
    i. Turn flow control to off; turn waste control to fill. Slowly turn on flow control until needle reads 0.5 to 0.65 range on pressure gauge. (explain procedure at each step to patient)
    ii. Give short initial fill (30 – 45 sec.); turn waste control to empty. This allows gas to escape from lower colon.
    iii. Alternately fill/empty colon watching Flow Control to register need to release by increase in the pressure reading or feed-back from the patient
    iv. On outflow cycle massage descending colon first; then start at Cecum with gentle massage and work around colon until release is complete
    v. Continue fill/release cycle until end of colonic. Treatment length is 30 to 45 minutes
h. To end colonic:
    i. Let patient know that treatment is finished
    ii. Explain to new patient that you will be removing the speculum: they will get off the table, sit on the toilet to complete release, put gown in hamper and get dressed. Inform them that an electrolyte (mineral) replacement drink is ready for them on the sink
    iii. Put on gloves. Take fresh paper towel; have patient roll onto left side. Slowly pull out speculum with tip angled up to prevent leaking; as you pull out speculum wrap in paper towel
i. Clean up:
    i. To remove hoses from machine hold speculum set-up below level of water inflow (to prevent leaking) and remove water inflow hose. Immediately hold it up to drain rest of water in water outflow hose
    ii. Hold up outflow hose to drain remaining water into machine. Remove hose and wrap hoses and speculum in pads from table. Discard in trash can.
    iii. Spray outflow pipe with cleaner, wipe and attach hose from Sanitizer. Turn on water flow until plastic view hose is filled; turn on disinfectant flow for ten seconds, then turn off. Turn off water flow.
    iv. Spray table with cleaner and wipe dry with paper towels
    v. Clean top and bottom of toilet seat and porcelain rim. Make sure sink and handles for water are clean and dry. Discard gloves.
    vi. Record the results of the treatment on Colonic form
    vii. Set up for next patient
j. End of Day:
    i. Turn off power to colonic machine and filter lights
    ii. Turn off water supply control under filter system
    iii. Empty hamper into laundry bags in physio area
    iv. Turn off over head lights

k. Once a month cleaning:
    i. Use a long handled brush w/ cleanser and liquid soap to thoroughly scrub plastic tube in machine (make sure to scrub metal parts at both ends)
    ii. Rinse brush and wrap in paper towel and store under sink

SCNM Medical Center Procedure:

Purpose of Procedure: To ensure the proper storage, control and dispensing of medications

Procedure Title: Storage, Control, Dispensing of Medications	**Procedure Number: 0050**
Department/Staff: Medical Center Employees	
Effective Date of Procedure: 9/10/10 **Procedure Updates**: 4/27/11	
Procedure Approved by: Executive Vice President of Academic and Clinical Affairs	**Signatures:**
Procedure Implemented by: Director of Clinical Operations	**Signatures:**

Procedure:

1. Medications are maintained at manufacturer recommended temperature.
2. Temperature logs are kept on a daily basis (See temp logs).
3. Approved personnel will check expiration dates weekly.
4. Medications are kept locked in appropriate areas.
5. Medications are accessed by approved personnel only.
6. Practitioners dispense medications per AZ Revised Statute.

SCNM Medical Center Procedure:

Purpose of Procedure: To motivate frequent and thorough hand washing by employees and to prevent the spread of infection.

Procedure Title: Hand Hygiene	**Policy Number: 0039**
Department/Staff: Medical Center Employees	
Effective Date of Policy: 9/10/10 **Policy Updates:** 8/22/12**,** 11/3/14	
Procedure Approved by: Medical Center Steering Committee	**Signatures:**
Procedure Implemented by:	**Signatures:**

Procedure:

A. Definitions
   1. ***Alcohol-Based Hand Rub-***an alcohol containing preparation designed for application to the hands for reducing the number of viable microorganisms on the hands. Preparations must contain >60 ethanol or isopropanol.
   2. ***Antimicrobial Soap-***Soap (detergent) containing substance that are applied to the skin to reduce the number of microbial flora (germs).
   3. ***Hand Hygiene-***a general term that applies to either hand washing with antibacterial or non antibacterial soap and water or the use of an alcohol based hand product.
   4. ***Hand Washing-***washing hands with plain soap and water.
   5. ***Plain Soap-***plain soap refers to detergents that do not contain antimicrobial agents.

B. Indications for Hand Hygiene
   1. After using the bathroom
   2. After touching animals
   3. Before and after preparing food
   4. Before and after eating
   5. After blowing nose
   6. After coughing or sneezing into hands
   7. Before and after treating wounds or cuts
   8. Hands must be washed immediately after removing gloves: gloves must be changed between contact with patients
   9. Before and after touching a patient
   10. After touching patient surroundings
   11. Before aseptic or clean procedures
   12. After being at risk of exposure to bodily fluids
   13. After handling garbage

C. Indications for washing hands with soap and water instead of alcohol based hand rub
   1. Before and after using the restroom
   2. Visible contamination of hands with blood, bodily fluids, and proteinaceous material
   3. Exposure of hands to spore forming organisms

D. Procedure for washing hands with soap and water
    1. Prepare paper towels.
    2. Turn on water and adjust the temperature. Avoid using hot water because repeated exposure to hot water may increase the risk of dermatitis
    3. Wet hands
    4. Apply soap
    5. Rub hand vigorously for 45-60 seconds. Scrub all surfaces including back of hands, wrists, between fingers and under fingernails.
    6. Rinse hands thoroughly under running water
    7. Dry thoroughly with disposable paper towels. Patting may be preferred to avoid irritation and dermatitis.
    8. Use paper towel to turn off faucet
E. Procedure for alcohol-based hand rub
    1. Apply a golf ball-sized application of alcohol-based solution to one palm and rub into opposite palm.
    2. Rub hands for up to 20 seconds covering all surfaces including back of hands, wrists, between fingers and under fingernails.
    3. Hands should be rubbed until dry.
F. Please refer to link below for visual information:
    http://www.who.int/gpsc/5may/Hand_Hygiene_Why_How_and_When_Brochure.pdf

SCNM Medical Center Procedure:

Purpose of Procedure: Priming Infusion Tubing

Procedure Title: Priming Infusion Tubing	**Procedure Number: 0025**
Department/Staff: Clinical Physicians/Clinical Students	
Effective Date of Procedure: **Procedure Updates:** 7/23/12, 9/12/14	
Procedure Approved by: Executive Vice President	**Signatures:**
Procedure Implemented by:	**Signatures:**

Procedure:

1. Compare the label to the physician's IV orders.
2. Inspect the IV solution for color. Examine for no cloudiness, no precipitation, or sediment. Ensure the outer package is free of damage or leaks.
3. Perform hand hygiene.
4. Apply clean disposable gloves.
5. Open infusion set while protecting sites from contamination.
6. Close the roller clamp.
7. Place insertion spike into IV solution bag while maintaining a sterile technique.
8. Hang IV solution on the IV pole.
9. Compress and release drip chamber until half full.
10. Slowly open the roller clamp and allow the fluid to flow through the tubing until it reaches the end. The protective end cap is to remain in place during this step. Ensure all air bubbles are removed.
11. Hang the IV tubing on the IV pole until ready to use. The protective end cap remains in place until ready for use.

Medical Center Procedures:

Purpose of Procedure: Isolation for the control of infection used to prevent infected patients from infecting others

Procedure Title: Isolation Procedure	**Procedure Number: 0061**
Department/Staff: Medical Center/PRC	
Effective Date of Procedure: **Procedure Updates:**	
Procedure Approved by: Executive Vice President	**Signatures:**
Procedure Implemented by: Chair of Infection Control Committee	**Signatures:**

Procedure:

Front Desk:

1. Schedule patient in Practice Management System as a same day appointment.
2. PSR will screen patient. Refer to form attached for questions.
3. Enter responses from questionnaire and requirements for isolation protocol into appointment notes and create an encounter note.
4. Scan questionnaire into patient's medical record uploading into the chart notes folder.
5. When scheduling appointments, instruct patient and persons who accompany them to inform PSR upon arrive and that we require the patient to wear a facemask as a precautionary measure. When scheduling the appointment, instruct patient and individuals who will be accompanying them to inform PSR upon their arrival prior to entering the building.
6. Inform supervising physician of schedule addition and that isolation protocols must be followed.
7. Once patient has arrived on campus, the patient will call the front desk from outside the building and the PSR will meet and give the patient a facemask to wear while in the Medical Center. Inform physician the patient has arrived and room the patient immediately.
8. Obtain flu kit from front desk and verify kit contents. Flu kit is to be left outside the room.

Physician:

1. Physicians/ students will follow sequence for putting on personal protective equipment (PPE). Instructions are located in each classroom.
2. Physician/student will enter exam room donned in PPE to begin intake. Leave cellphone and laptops in classroom.
3. Upon completion of intake, physician/student will disrobe PPE into designate trash bin. Exit immediately to report to supervising physician.

4. Determine risk for possible flu/Enterovirus/Ebola infection.
5. If Ebola, report to the Health Department: 602-542-1025
6. Physicians and students will follow sequence for putting on personal protective equipment (PPE) before reentering exam room. Instructions located in each classroom
7. Call lab from exam room informing them patient will need a nasal swab. Indicate which test will need to be processed.
8. Treatment Plan will be reviewed with patient.
9. Call Medicinary to place order for supplements. Payment will be taken over the phone. Medicinary staff will deliver supplement outside of exam room.
10. Call check out at 133 or 140 and have PSR enter CPT and ICD codes, collect payment for visit over the phone.
11. Schedule follow-ups as phone consults.
12. Disrobe PPE into designated trash prior to exiting room.
13. Escort patient out of Medical Center. Mask is to remain on patient until exit. Patient may dispose in waste receptacle outside of Medical Center.

Medicinary:

1. Gather supplements requested from physician or student.
2. Enter in Point of Sale.
3. Call exam room to collect payment over the phone. If patient is using cash, the student or physician will deliver payment to Medicinary.
4. Bag supplements with receipt and change if necessary. Place bag outside of exam room for patient.

Flu Questionnaire

Patient Services Questionnaire for Ebola/Influenza/Measles screening:

Caller Name: _____

Phone Number: _____

Date of Birth: _____

Patient Services Rep: _____

If a patient calls in regards to cold or flu-like symptoms please ask them the following questions.

1. Have they traveled internationally or flown in the last 3 weeks?
2. Ask patient the list of the symptoms and circle all of them that apply;
    a. Fever-
        i. How high?
        ii. How long?
    b. Cough-
        i. If yes, how long has it been present?
    c. Sore throat
    d. Headache
    e. General weakness
    f. Muscle pain
    g. Vomiting
    h. Diarrhea
    i. Abnormal bleeding
    j. Asthma-like symptoms or history of asthma
3. Action-Circle one:
    a. Refer to Resident on call for further screening
    b. Scheduled at Medical Center?
        i. Physician, Date and time of appointment:_____
        ii. Physician notified of isolation protocol:_____

SCNM Medical Center Procedure:

Purpose of Procedure: Define medical, biohazardous and sharps waste and the process by which waste is disposed

Procedure Title: Medical Waste Management	**Procedure Number: 0040**
Department/Staff: Medical Center Employees	
Effective Date of Procedure: 9/10/10 **Procedure Updates:**	
Procedure Approved by: Executive Vice President of Academic and Clinical Affairs	**Signatures:**
Procedure Implemented by: Director of Clinical Operations	**Signatures:**

Procedure:

Definitions:

Medical Waste is defined in the Medical Waste Management Act as biohazardous or sharps waste and waste which is generated or produced as a result of the:

- Diagnosis, treatment, or immunization of human beings/animals;
- research pertaining to the diagnosis, treatment, or immunization of human beings/animals;
- production/testing of biologicals;
- the accumulation of properly contained home-generated sharps waste; or the removal of trauma scene wastes.

Biohazardous Waste is defined as:

1. Laboratory waste, including, but not limited to, all of the following:
   - Human or animal specimen cultures from medical and pathological laboratories.
   - Cultures and stocks of infectious agents from research and industrial laboratories.
   - Wastes from the production of bacteria, viruses, spores, discarded live and attenuated vaccines used in human health care or research, discarded animal vaccines, including Brucellosis, Contagious Ecthyma, as identified by the department, and culture dishes and devices used to transfer, inoculate, and mix cultures.
2. Human surgery specimens or tissues removed at surgery or autopsy, which are suspected by the attending physician and surgeon or dentist of being contaminated with infectious agents known to be contagious to humans.
3. Animal parts, tissues, fluids, or carcasses suspected by the attending veterinarian of being contaminated with infectious agents known to be contagious to humans.
4. Waste, which at the point of transport from the generator's site, at the point of disposal, or thereafter, contains recognizable fluid blood, fluid blood products, containers, or equipment containing blood that is fluid or blood from animals known to be infected with diseases which are highly communicable to humans.

5. Waste containing discarded materials contaminated with excretion, exudate, or secretions from humans or animals who are required to be isolated by the infection control staff, the attending physician and surgeon, the attending veterinarian, or the local health officer, to protect others from highly communicable diseases or diseases of animals that are highly communicable to humans. Biohazardous materials covered by this program may include:

- Infectious organisms that can cause disease in humans or cause significant environmental or agricultural impact Human or primate tissues, fluids, cells, or cell cultures;
- Animal tissues, fluids, cells, or cell cultures that have been exposed to infectious organisms;
- Recombinant DNA in vitro, in vivo, and in clinical trials
- Transgenic plants or animals;
- Human gene transfer clinical trials Releases of recombinant DNA to the environment
- Animals known to be reservoirs of zoonotic diseases; and Select Agents.

Sharps waste is defined as any device having acute rigid corners, edges, or protuberances capable of cutting or piercing, including, but not limited to, all of the following:

- Hypodermic needles, hypodermic needles with syringes, blades, needles with attached tubing, syringes contaminated with biohazardous waste, acupuncture needles, and root canal files.
- Broken glass items, such as Pasteur pipettes and blood vials contaminated with biohazardous waste.
- Any item capable of cutting or piercing that is contaminated with trauma scene waste.

MEDICAL WASTE DOES NOT INCLUDE:

- Waste generated in food processing or biotechnology that does not contain an infectious agent.
- Waste generated in biotechnology that does not contain human blood or blood products or animal blood or blood products suspected of being contaminated with infectious agents known to be communicable to humans.
- Urine, feces, saliva, sputum, nasal secretions, sweat, tears, or vomitus, unless they contain fluid blood.
- Waste which is not biohazardous, such as paper towels, paper products, articles containing non-fluid blood, and other medical solid waste products commonly found in the facilities of medical waste generators.
- Hazardous waste, radioactive waste, or household waste.
- Waste generated from normal and legal veterinarian, agricultural, and animal livestock management practices on a farm or ranch.

Procedure:

Dry Biohazardous or Medical Waste:

- Collect dry waste in red biohazard bags
- Label bags, if not preprinted with the following information before adding waste:
    - International biohazard symbol and the word “Biohazard”
- Tie or tape bag closed
- Take the sealed bag to the dirty utility room or biohazardous waste collection site for a waste pickup

Liquid Biohazardous or Medical Waste:

- Dilute liquid waste with Cavicide
- Let sit for at least 20 minutes before pouring down drain

Disposal of Biohazardous Sharps:

- Place Sharps in a rigid, leak proof, puncture resistant container.
- Label sharps container, if not preprinted with the following information before adding sharps:
    - International biohazard symbol and the word "Biohazard"
- Do not place free liquids such as full syringes in sharps containers •
- Take the sealed sharps container to the dirty utility room or biohazardous waste collection site for waste pickup

Taken from University of California, Merced

SCNM Medical Center Procedure:

Purpose of Procedure: To ensure safe medication dispensing following the guidelines within the Arizona Administrative Code R9-10-Article-10

Procedure Title: Medication Dispensing	**Procedure Number: 0058**
Department/Staff:	
Effective Date of Procedure: **Policy Updates:** 10/23/2014	
Procedure Approved by: Medical Center Steering Committee	**Signatures:**
Procedure Implemented by:	**Signatures:**

Procedure:

Clinician:

1. A patient's medications are reviewed with each visit to ensure that it meets the patient's needs. All medications are documented under the meds tab in the EHR, including the medication that is dispensed.
2. The patient's allergies are verified and update in EHR with each visit. Document completion of this step in the HPI section of the EHR
3. Medications to be dispensed are reviewed for interactions with the patient's current medication regimen through the medications tab in the EHR.
4. Medications covered under this policy are dispensed with written prescription by a physician who has a certificate to dispense.
5. The written prescription must include:
   - Patient name
   - Date of birth
   - Medical record number
   - ICD-9
   - Name of the medication
   - Route, dosage and how the medication should be taken
   - Number to dispense
   - Number of refills
6. The patient is given the option to have the medication dispensed from SCNM Medical Center or a pharmacy of their choice
7. If dispensing oral medication from SCNM Medical Center the following paperwork is required:
   - Service summary for urgent care medication signed by the physician– an original and a copy
   - Patient service summary signed by the physician

Dispensing Staff:

1. Only appropriately trained staff with access to Apothica's web based dispensing program are to dispense oral medications

2. Medication that is dispensed with a prescription must be properly labeled with:
    - Date it was dispensed
    - Patient name
    - Date of birth
    - Prescribing physician's name, address, and telephone number
    - Name of the medication
    - Route, strength, dosage and how the medication should be taken
    - Number to dispense
    - Number of refills
    - Expiration date
3. A medication information handout is provided and reviewed with the patient. The information handout provided includes:
    - Indication for the medication
    - How to take the medication
    - The anticipated results of taking the medication
    - Potential adverse reactions
    - Potential side effects
    - Adverse reactions that could occur if the medication is not taken as prescribed
4. Any sample medication provided to the patient must include:
    - Name
    - Strength
    - Dosage
    - Amount
    - Route of administration
    - Expiration date
5. Prior to dispensing, verify with the patient their information and allergies in web based dispensing program is correct.
6. A two person independent verification is completed, verifying the medication being dispensed is the medication that is prescribed.
7. Ensure the patient knows to contact the clinic if any adverse reactions occur. PSR is to notify the prescribing physician. If that physician is not available the resident on call will be notified.

SCNM Medical Center Procedure:

Purpose of Procedure: Ensure safe medication storage and management following the guidelines within the Arizona Administrative Code R9-10-Article-10

Procedure Title: Medication Management and Storage	**Procedure Number: 0050**
Department/Staff:	
Effective Date of Procedure: **Policy Updates**: 9/25/2014	
Procedure Approved by: Medical Center Steering Committee	**Signatures:**
Procedure Implemented by:	**Signatures:**

Procedure:

1. When medication is received from the distributor, the quantity and expiration dates are entered into web based inventory system.

2. Medication is placed in the designated locked storage.

3. Other than when dispensing, designated medication storage must remain locked at all times.

4. Stock is rotated when a new shipment is received, placing items closest to expiration in front.

5. Weekly inventory is completed and documented.

6. Any expired medication is recorded and disposed of following hazardous material guidelines in the appropriate disposal container.

7. Inventory and expired medication documentation is kept in the medication management binder located in the IV room.

SCNM Medical Center Procedures:

Purpose of Procedure: Regulating Intravenous Flow Rate

Procedure Title: Regulating Intravenous Flow Rate	**Procedure Number: 0027**
Department/Staff: Clinical Physicians/Clinical Students	
Effective Date of Procedure: **Procedure Updates:** 5/15/12, 11/3/14	
Procedure Approved by: Executive Vice President	**Signatures:**
Procedure Implemented by:	**Signatures:**

Procedure:

1. Verify physician's IV order.
2. Observe patency of the IV line after established per standard procedure.
3. Inspect site and verify with patient how insertion site feels.
4. Know calibration in drops per milliliter of specific infusion set. (Found on the package of the IV tubing.
5. Calculate drops per minute (gtt/min).
    - $\frac{\text{Total volume x IV tubing calibration/constant}}{\text{Time of infusion}}$
6. Calculate hourly rate in milliliters per hours (ml/hr)
    - $\frac{\text{gtt/min}}{15} \times 60$
7. Time flow rate by a watch.
8. Monitor infusion rate as needed.

SCNM Medical Center Procedure:

Purpose of Procedure: To protect the safety of Patients, Students, Employees, Doctors

Procedure Title: Suicidal Patients & Involuntary Holds	**Procedure Number: 0032**
Department/Staff: Medical Center Employees	
Effective Date of Procedure: **Procedure Updates:** 2/11/2015	
Procedure Approved by: Executive Vice President	**Signatures:**
Procedure Implemented by:	**Signatures:**

If a patient is suicidal due to an existing and documented mental disorder (DSM classification), or threatens to kill themselves or others, SNMC will follow procedure listed

Procedure:

Voluntary Evaluation

1. Patient should be asked if they will voluntarily go to the Maricopa Medical Center for evaluation
2. If patient agrees – arrange for transportation and call MIHS ER (602-344-1945) and let the psychiatric unit know the patient is on the way

Patient refuses evaluation – Petition Process

1. Call MIHS @ 602-344-1945 and speak with a mental health coordinator (someone is available 24 hours a day)
2. Inform them of the situation and request a petition for evaluation to be faxed to 480-970-0003 ASAP
3. Fill out the petition and fax it back to the number listed
4. Keep the patient at the Medical Center. If this is not possible, let the MIHS mental health coordinator know, and they will give you instructions
5. The petition will be reviewed by MIHS personnel and a decision will be made as to whether to transport, or not. This may necessitate additional phone conversations with the attending physician at the Medical Center.
6. Once the decision has been made to transport, MIHS will contact the local police department to arrange for the patient to be picked up
7. MIHS will then evaluate the patient and decide if admission is necessary

The incident and all phone conversations must be reported and documented.