HIPAA PROCEDURES MANUAL

Dr. Robert L. Ruxin

9-23-13
Updated 4-5-2021

This document contains the procedures to be followed by all workforce members and contractors Dr. Robert L. Ruxin 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 Karin Halstead Privacy Official.

Table of Contents

Privacy Procedures

Privacy Official Job Description

Actions to be taken for the privacy official job description

1. Karin Halstead has been appointed as Dr. Robert L. Ruxin's, "privacy official". The privacy official will be responsible for completing the job description for the privacy official.

2. The privacy official has met with the Dr. Robert L. Ruxin to review the HIPAA Privacy rule and to determine the responsibilities of the privacy official.

3. Dr. Robert L. Ruxin has agreed to the following job description.

PRIVACY OFFICIAL JOB DESCRIPTION

Job Title:

Privacy Official

Job-Sharing? No, this job is performed by the Practice Manager

Job Description:

The privacy official is responsible for implementing and maintaining this practice's HIPAA Privacy requirements.

Reporting structure:

The privacy official reports directly to Dr. Robert L. Ruxin

Job Duties:

1. Develop, implement and maintain this practice's HIPAA Privacy and Security policies.
2. Periodically review and audit this practice's HIPAA Privacy policies and procedures updating these where appropriate to respond to patient complaints or changes affecting the implementation of privacy policies and procedures.
3. Develop, implement and maintain this practice's HIPAA Privacy and Security procedures and forms.
4. Develop and implement this practice's HIPAA records filing system.

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

22. Ensure that records are retained in accordance with this practice's records retention procedure.
23. Handle all workforce training and awareness programs in HIPAA Privacy and Security requirements in accordance with this practice's workforce training procedure.
24. Handle all workforce sanctions where any member of this practice's workforce intentionally or unintentionally violates any of this practices privacy or security policies.
25. Ensure all business associates are identified and have signed business associate agreements in accordance with this practice's business associate policy.
26. Cooperate with any privacy investigation by the Department of Health and Human Services.
27. Handle any other privacy and security practice as defined in this practice's Notice of Privacy Practices.

Implementing the HIPAA records filing system

Actions to be taken for records filing

1. **Karin Halstead** has been appointed as the Dr. Robert L. Ruxin "privacy official". The privacy official will be responsible for developing and maintaining a HIPAA records filing system.

2. The privacy official have met with Dr. Robert L. Ruxin to review the filing system procedures.

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

4. 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 form.

5. In collaboration with the Dr. Robert L. Ruxin implement a separate medical record for psychotherapy notes.

6. Establish a locked file in your office for all HIPAA records.

7. 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.

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

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

10. File the Workforce Training Log and any other training logs or questionnaires in a separate file titled "HIPAA training".

Actions To Be Taken For All Access Requests

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

2. Forward all requests for access or copying of protected health information to Karin Halstead, Dr. Robert L. Ruxin's "privacy official."

3. During the initial contact (or as soon as possible after the initial contact), inform the patient or their personal representative that this organization requires that the request be submitted using our Request for Access to Protected Health Information form. Provide the patient with a copy of this form either in person or by mail or fax. If the patient expresses concerns about completing a form, invite them to visit so you can assist them in completing the form.

4. Contact the patient (or his or her representative) within 30 days of receiving the written request. This contact will be to verify receipt of the request and it will be done in person or by telephone

5. Track the status of the request on the submitted Request for Patient Access to Protected Health Information form.

6. Review the request form as soon as it has been received. This review will determine:

    - The exact amount and nature of information requested, and where that information is kept.
    - Whether the requestor requires access, copies of the information, or a summary of the information or some combination.
    - The format of the requested records.
    - The format of the requested copies, if any.

    Complete the review within 30 working days of receipt of the request form.

7. If the information requested is not kept by this organization but you can determine where the information is kept, direct the individual to the appropriate organization.

8. Review the access request and determine if the request will be granted or denied. Document the grant or denial of access in the evaluation section of the Request for Access to Protected Health Information form. Send a copy of the evaluation section to the requestor by certified (receipt) mail. A request for access may only be denied for the following reasons:

    - The requested information includes psychotherapy notes ("process notes not included in the medical record"). (non-reviewable).
    - The requested information is covered under the clinical laboratory improvement amendments. (non-reviewable).
    - The requested information was compiled in anticipation of or for use in a civil, criminal, or administrative proceeding. (non-reviewable).
    - An organization that is a correctional institution or is functioning on their behalf may deny access to inmates. (non-reviewable)
    - The information was obtained in the course of research that is in progress (non-reviewable)
    - The records are subject to the Privacy Act (see your privacy official if you have questions. This reason is non-reviewable)
    - The information was obtained by someone other than a health care provider under a promise of confidentiality and releasing it may reveal the source (non-reviewable)
    - A licensed health care professional has determined, in the exercise of professional judgment, that the access may endanger the individual or someone else. (reviewable)
    - The information refers to another person (other than a licensed health care provider) and the provider has determined in professional judgment that the other person may be substantially harmed. (reviewable)
    - A personal representative made the request and a licensed health care provider has determined in the exercise of professional judgment that the provision of access is reasonably likely to cause substantial harm to the individual or someone else. (reviewable)

9. If the decision is made to grant the request, proceed to the "Actions to be Taken When an Access Request is Granted" procedure, below. Otherwise proceed to the "Actions to be Taken When an Access Request is Denied" section.

Actions To Be Taken When An Access Request Is Accepted

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

2. Ensure that the response clearly states the charges incurred for copying or summary preparation (if any) and that payment must be made prior to or at the time of the access.

3. If the request is granted, determine a convenient time for access within 30 days of approval of the request. (Or at the earliest time convenient to the requestor.) The access *must* be granted within 30 days of the receipt of the request form.

4. Arrange for any records copying or transfer within 30 days of receipt of prepayment. In any case, any records copying or transfer *must* be completed within 30 days of receipt of the request form.

5. Calculate the total amount to charge for processing the request. This practice will charge $.50 per page for copies of the information requested, plus $5 per quarter hour for clerical time to facilitate this copying. This organization will also charge the value of postage used (if any) for preparations of summaries of protected health information, if a summary is requested.

6. Be present when the patient or their personal representative appears at the scheduled time and at all times when the requestor is reviewing any original records.

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

Actions To Be Taken When An Access Request Is Denied

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

2. Ensure that the requestor is granted access to all information that is not subject to the grounds for the denial.

3. Determine if the grounds for denial are reviewable or not (a notation to that effect is in the determination step of the Actions to be Taken When Initially Processing an Access Request Procedure and inform the requestor of your findings.

4. Arrange for a review of denied inspection requests if the patient or their personal representative requests such a review. This review will be conducted by Dr. Robert L. Ruxin or another licensed health care professional who did not participate in the original review and denial.

5. Act only on review requests that are documented in writing. You may require the patient to complete a new Request for Patient Access to Health Information for this purpose, or you may have the patient add the review request to the original form.

6. Arrange for this review to be completed promptly after receipt of the review request.

7. Instruct the reviewer to document the results of the review in the review section of the Request for Access to Protected Health Information form.

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

Actions To Be Taken For All Amendment Requests

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

2. All requests for amendment will be forwarded to Karin Halstead, the Dr. Robert L. Ruxin's privacy official.

3. Contact the patient (or his or her personal representative) who requests an amendment within 30 days of the request. Inform the patient or their personal representative that this practice requires the request be submitted using our Request for Amendment form. Provide the form in person, by mail, or by fax. If the requestor expresses concerns about completing a form invite them to visit so you can assist them in completing the form.

4. Track the status of each request in the evaluation section of the Request for Amendment form.

5. Schedule a time for the patient or their personal representative to visit the practice and inspect the medical record if so needed (see "Access Request Processing.

6. Review the amendment information stated on the Request for Amendment form. Meet with the Dr. Robert L. Ruxin to review the amendment

7. Determine whether to accept or deny the amendment. **Note: An amendment may be denied only for one of the following four reasons:**

    - **the information is accurate and complete as it is,**
    - **the information did not originate at this organization,**
    - **the organization is not part of a set of records for making decisions about the patient or**
    - **the information is not available for inspection for some other reason.**

    Record your decision in the evaluation section of the Request for Amendment form.

8. Forward a copy of the evaluation section of the Request for Amendment form to the patient within 60 days of completion, by certified receipt requested mail.

9. Forward a copy of the evaluation section of the Request for Amendment and a copy of the initial Request for Amendment to our professional liability carrier's risk management contact.

Actions To Be Taken When the Amendment Request Is Accepted

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

2. Insert the amendment into the medical record with an alert flag to indicate the record has an amendment (chart) in a special section.

3. Send a copy to the individuals or entities that the patient or the patient's personal representative has requested to be notified (if any).

4. Send a copy of the amendment to any other entities or business associates who may have received the incorrect information.

5. Notify appropriate staff of the amendment to ensure that accurate information is disclosed from this point forward.

6. File the original request and the response in this organization's HIPAA compliance file.

Actions To Be Taken When An Amendment Request Is Denied

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

2. Ensure that the denial of amendment includes a statement of the requestors rights:
    - To request that the proposed amendment be included in all future disclosures
    - To file a statement of disagreement
    - To complain to the organization or to the department of health and human services

3. File the original request and the response in this organization's HIPAA compliance file.

4. If the requestor files a statement of disagreement with the denial, file the statement with the original request and the response.

5. If the requestor files a statement of disagreement with the denial, compose a rebuttal using the rebuttal section of the Request for Amendment form and file it with the statement of disagreement. Provide a copy of the rebuttal to the requestor

Actions To Be Taken For All Complaints

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

2. Inform Karin Halstead**,** Dr. Ruxin's, privacy officials immediately whenever you receive a privacy complaint from a patient or the patient's personal representative. Include, at a minimum:

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

3. In addition to these reporting steps, send an interoffice "memo" as soon as possible after receiving the complaint to the privacy official to document the fact that a complaint was made

4. Contact the patient making the complaint within 30 days of receiving notice from the staff. Contact them using the most efficient and immediate means available, preferably verbally, by telephone. Document the date and time of their response. If a voice mail is left, continue to pursue direct communication until it occurs.

5. Alert staff that a complaint has been filed and reiterate to all members of the workforce they should refrain from any retaliation or intimidation against the individual complaining.

6. Request that the patient complete a written complaint form (if the original complaint was verbal or written in non-standard format). This form can be mailed to the patient after the initial conversation, however request the patient come to the office for a face to face communication with you so you can complete or modify the written report.

7. File the completed complaint 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 Is Found

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

2. If you determine that there has been no violation of this organization's privacy policies, then document these findings on the complaint form. (*IMPORTANT: If, in the course of investigating the privacy complaint, you determine that the complaint is related to clinical or medical care, report the situation immediately to our professional liability carrier as an incident.)*

3. Meet with the patient and explain your findings; also provide the patient with a written record of the complaint resolution.

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

5. If the patient is dissatisfied with the disposition of his or her complaint, refer this matter to

   - our professional liability carrier as part of their early warning program;
   - our legal counsel; and
   - the physician partner in charge.

Actions To Be Taken When A Compliance Violation Is Found

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

2. If you determine that a violation of this organization’s privacy policies has occurred, document this fact on the complaint form.

3. Meet with Dr. Robert L. Ruxin as soon as possible to review the violation and develop a remediation plan. Document the remediation steps on the complaint form and an action plan established to complete them. Advise the appropriate workforce members or other persons (if any) who bear responsibility for privacy policy violations and impose the appropriate sanctions on responsible personnel. (*IMPORTANT: If, in the course of investigating the privacy complaint, the privacy official determines that the complaint is related to clinical or medical care, report the situation immediately to our professional liability carrier as an incident.)*

4. Meet with the patient and explain your findings; also provide the patient with a written record of the complaint resolution.

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

6. If the patient is dissatisfied with the disposition of his or her complaint, refer this matter

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

    - to our legal counsel; and

    - to the physician partner in charge.

7. Report to Dr. Robert L. Ruxin on a weekly basis to report the status of the remediation plan until all corrective activities have been accomplished.

Actions To Be Taken For All HPAA 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.

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. Karin Halstead HAS REVIEWED THIS PROCEDURE TO ENSURE THAT IT CONFORMS TO THE GUIDANCE PROVIDED BY OUR PROFESSIONAL LIABILITY INSURANCE CARRIER. THE PRIVACY AND/OR SECURITY OFFICIAL WILL PERFORM ALL OF THE FOLLOWING STEPS.

2. This medical practice has trained all staff, including physicians, to immediately notify the Privacy and Security Officials upon receipt of a notice of a HIPAA investigation. The actual notification will immediately be forwarded to the Privacy and Security 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 and Security Officials will meet with senior management [physician in charge]/[practice administrator] to review the contents of the notice. Determine if you will seek legal counsel before proceeding

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

6. Begin an internal investigation to review the incident

7. Notify any staff members who may be part of the review that you are investigating a possible HIPAA violation and their cooperation is needed.

Reiterate that their cooperation with you or the HHS agency will not result in any retaliation against them.

8. Throughout your 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 your 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 your internal investigation including any interviews with staff members. If you determine a violation has occurred or a gap in your compliance exists, immediately correct this gap with corrective measures and document how you have done so.

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

11. If a member of your workforce has violated policies and procedures, follow your sanction procedures. Be sure that your sanctions are well documented and cannot be construed as retaliation.

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

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

Confidential Channel Communication Request Processing

Actions To Be Taken For Confidential Communication Requests

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

2. All requests taken by staff or the physicians will be forwarded to Karin Halstead the privacy official for handling.

3. Ask the patient or personal representative who requests an alternate confidential communication channel will be asked to complete the "Confidential Channel Communication Request" form.

4. If there is sufficient time, attempt to review the completed form while the patient is still present. If not, inform the requestor that the privacy official will review the form and contact the patient within 30 days.

5. Review the request and decide if it will be granted or not. The HIPAA requirements are:

    - This organization may decide what is "reasonable". This organization may condition the provision of a reasonable accommodation when appropriate, based on information as to how payment, if any, will be handled; and the specification of an alternative address or other method of contact (without these we may deny the request).
    - If this organization is a health care provider and it can reasonably accommodate the confidential channel, the channel *must* be granted (a provider may not require an explanation of why the requestor is asking for a confidential channel).
    - If this organization is a health plan and it can reasonably accommodate the confidential channel *and* the requestor states that they would be endangered if the information were disclosed to the wrong person, the channel *must* be granted.

6. As soon as possible after deciding to grant or deny the request, inform the requestor of your decision and provide them with a copy of the grant or denial in writing. 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 page.

7. If the request is granted, place one copy of the Confidential Channel Request/Response form in the patient's medical record under a separate tab. Place an alert in the notes section of the patient's electronic chart to indicate that an alternate communication channel is in effect. File an additional copy in this organization's HIPAA Compliance file. (Each request makes all previous requests obsolete.) The patient must be made to understand that the new form should contain all confidential channel communications requests that are to be in effect–not just the most recent request. Old confidential channel communications request forms are to be kept in the HIPAA compliance file for a period of six years past the date on which they were last in effect.)

8. If the request is granted, meet with the appropriate workforce members to ensure that the request is implemented in their operational activities.

Disclosure Accounting Request Processing

Actions To Be Taken For Disclosure Accounting Requests

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

2. Forward all requests for disclosure accounting to Karin Halstead the privacy official.

3. Contact the patient or personal representative who requests a disclosure accounting within 30 days of the request. Inform the patient or their personal representative that this practice requires the request be documented and submitted using our Request for Accounting of Disclosures of Protected Health Information form. Provide the requestor with a copy of the form, and if the requestor expresses concerns about completing the form invite them to visit so you can assist them in completing the form.

4. Review the request form. This review will verify that the accounting is valid and for health information disclosures that are required to be accounted by HIPAA. Those disclosures are everything but:
   - Disclosures made to carry out treatment, payment and health care operations.
   - Disclosures made to individuals (patients or health plan members).
   - Disclosures made for the facility's directory or to persons involved in the individual's care.
   - Disclosures made for national security or intelligence purposes.
   - Disclosures made to correctional institutions or law enforcement officials.
   - Disclosures that occurred prior to the compliance date for this organization.

5. Review the request and determine if a law enforcement official has requested that disclosures to the law enforcement organization not be included in an accounting of disclosures at this time. If so, omit the relevant disclosures from the disclosure accounting.

6. Review the records and compile a list of every disclosure for the past six years subject to an accounting. Ensure that each entry contains:
   - The date of the disclosure

- The name of the entity or person who received the protected health information and, if known, the address of such entity or person
- A brief description of the protected health information disclosed
- A brief statement of the purpose for each disclosure

7. If many disclosures were made to the same entity for the same purpose, it is permissible to group them together by providing the following:
   - The information provided in step 5 above.
   - How frequently or how many times the information was disclosed.
   - The date of the last such disclosure.

8. File the request and the disclosure accounting provided to the requestor in the organization's HIPAA compliance file.

Individual Permission—Authorization

Actions To Be Taken When Obtaining Written Authorization

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

2. Obtain an authorization form that matches the type of disclosure that will be made (for example, "pre-employment physical," "transfer of records," "clinical research participation," etc.).

2. Confirm the identity of the person who will sign the authorization (if not known). If the person who will sign the authorization is a personal representative, confirm his or her relationship to the patient.

3. Complete all parts of the particular authorization form that need to be completed (expiration date, etc.).

4. Provide a copy of the signed authorization to the individual or personal representative.

5. File a copy of the completed authorization in the patient's chart.

Actions To Be Taken When Obtaining Verbal Agreement

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

2. 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.

3. Whenever a patient arrives with a family member or friend who is not a personal representative, ask the patient if the patient gives permission for the staff to inform the family member or friend of the patient's condition or to share other information concerning the patient.

4. If the patient provides verbal agreement, document this in the medical record. Record this under the HIPAA tab in the electronic medical record and titled "family or friends granted permission". Include the date, time, name, and telephone number of the family or friend in the record, as appropriate.

5. Do not discuss or disclose any information pertaining to the patient to any individual who has not been granted permission and documented.

Information Disclosures--Minimum Necessary

Actions To Be Taken For All Information Disclosures

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

2. Determine whether or not the disclosure requires an authorization signed by the patient (or the patient's personal representative). All disclosures except the following must be authorized:

    - To the individual (patient or health plan member) himself or herself, or to a personal representative of the individual (that is, to a person who has a legal relationship with the individual that establishes a right to make decisions concerning the health care of the individual).
    - To demonstrate compliance with HIPAA regulations. (cooperation with the Department of Health and Human Services when it conducts compliance reviews or investigates complaints).
    - To cooperate with courts, public health authorities, law enforcement agencies or for other “public purposes.”
    - For treatment, payment or health care operations.
    - For facility directories or to persons involved in the care of the individual, (provided that the individual has been given the opportunity to object to such disclosures).

3. Disclose only the minimum amount of information necessary to accomplish the purpose of the disclosure. Do *not* disclose an entire medical record unless an entire medical record is the minimum amount of information needed to accomplish your purpose. (Note: The "minimum necessary" rule does not apply to:

    - Uses or disclosures for treatment purposes.
    - Disclosures to the Department of Health and Human Services for compliance review or complaint investigation purposes.
    - Disclosures to the individual (or to the individual's personal representative) concerning PHI that pertains to the individual.
    - Disclosures authorized by the individual.

- Disclosures that are required by law.
- Disclosures necessary for HIPAA compliance.)

4. If the disclosure is to anyone who is unknown to you, determine first their name, function and authorization to access the information. Acquire copies of any necessary documents or permissions. (If the disclosure is to a personal representative, ensure that the relationship of the individual to the patient is valid. (See the procedure on dealing with personal representatives.) Be aware of any restrictions on the individual's authority to obtain patient information.) You are not required to ensure that such documents are not forgeries. If they appear to be valid, you have met your obligation. For example: you may rely on written statements on appropriate government agency letterheads. You may also rely on the presentation of identification badges or other official credentials.

5. If this disclosure is pursuant to an authorization signed by the individual or a personal representative of the individual, ensure that the authorization is valid. To be valid, an authorization must include:

    - A description of the information to be disclosed. (Do not disclose information beyond the bounds of this description.)
    - Dr. Robert L. Ruxin specifically named as being authorized to disclose the information.
    - The name of the person or organization specifically authorized to receive the information.
    - A description of the purpose for which the information will be disclosed. ("At the request of the individual" is sufficient purpose if the individual has initiated the authorization.) Note: This must be a single purpose; compound authorizations are not valid.
    - An expiration date or expiration event.
    - Signature of the individual to whom the information pertains. (If signed by a personal representative, a statement of the representative's authority to act on the individual's behalf must be included.)
    - The date on which the authorization was signed.

6. Determine whether or not the disclosure is "accountable." If so, make an entry in the disclosure accounting log. All disclosures are accountable except:

    - Disclosures made to carry out treatment, payment and health care operations.
    - Disclosures made to individuals themselves (or to personal representatives of the individuals).

- Disclosures that were authorized by the individual (or the individual's personal representative).
- Disclosures made for the facility directory purposes or to family, friends or other persons involved in the individual's care.
- Disclosures made for national security or intelligence purposes.
- Disclosures made to correctional institutions or law enforcement officials.
- Disclosures of limited data set information.
- "Incidental" disclosures (that is, unintended disclosures that occur in the course of making disclosures allowed by HIPAA).
- Disclosures that occurred prior to the compliance date for this organization.

Actions To Be Taken When Making Routine Disclosures Of Information

Actions To Be Taken When Making Non-Routine Disclosures

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

2. Identify the purpose for which the disclosure will be made. Be as specific as possible. (For example, a business associate may suspect that some information that it maintains is incorrect and wants to "compare notes" with someone whom it believes has more up-to-date information.)

3. Identify the items of information required. Be as specific as possible. (For example, the results of a particular test performed on a particular day.)

4. For each item identified in the previous step, consider the effect of removing it from the disclosure. That is, think about whether the purpose of the disclosure would or would not be satisfied if the item were removed. If the purpose of the disclosure may be satisfied without the information, do not disclose the information.

5. Consider whether or not you should obtain an authorization from the individual to whom the requested information pertains.

Actions To Be Taken When Disclosing Information to Law Enforcement

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

2. Disclose information if the disclosure is required by law. (Contact Karin Halstead if you are not sure whether this particular disclosure is "required by law." Karin Halstead will contact our legal counsel if necessary.)

3. Do *not* disclose any information about an individual committing a crime if the information was obtained while the individual was seeking or undergoing treatment to reduce his or her tendency to commit the crime.

4. If the individual admits to participating in a crime or if the law enforcement official asks for help in identifying the perpetrator of a crime, you may only disclose the following information to the law enforcement authorities (except as required by a court order):
   - name and address
   - date and place of birth
   - social security number
   - ABO blood type and Rh factor
   - date and time of treatment
   - type of injury
   - date and time of death (if applicable)
   - description of distinguishing physical characteristics (height, weight, gender, hair, etc.)

5. Do *not* disclose DNA or DNA analysis information, blood or tissue samples, analyses, or typing results to law enforcement authorities unless required to do so by a court order.

6. Disclose information about the victim of a crime to law enforcement authorities only if:
   - The victim agrees
   - In the event of the victim's incapacity, the law enforcement official states that the information is needed for an immediate law enforcement activity, is needed to determine if a violation of law has been committed by someone other than the victim, is not to be

used against the victim, and the disclosure is in the best interests of the victim (as decided in the professional judgment of the health care provider)

7. In the event the crime occurred on the premises, disclose all necessary and relevant information.

8. Report abuse, neglect, or domestic violence only if the victim agrees, the disclosure is required by law, or the disclosure is allowed by law and is necessary to prevent further harm.

9. If the crime reported is one of abuse, neglect, or domestic violence, you *must* inform the individual that you have reported their information to law enforcement, *unless* a licensed health care provider, in their professional judgment, determines that doing so would endanger the individual.

Actions to Be Taken When Disclosing Information to Correctional Institutions and Other Law Enforcement Custodial Situations

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

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. Document all disclosures covered in this section in the patient's medical record, if appropriate, as well as in the Disclosure Accounting Log.

Actions To Be Taken When Disclosing Information To Public Authorities

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

2. Disclose all information required by law.

3. Disclose information about victims of abuse only to the appropriate authorities and only if the individual agrees; reporting is required by law; or reporting is allowed by law and is necessary to prevent further harm.

4. If you report abuse, neglect, or domestic violence to the authorities, you *must* inform the individual that you have done so *unless* a licensed health care provider, in their professional judgment, determines that doing so could endanger the individual.

5. Disclose information to avert a serious threat to health or safety only to those able to prevent or reduce the threat and only as necessary.

Actions To Be Taken When Disclosing Information For A Judicial Or Administrative Proceeding

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

2. If you are presented with a court order, grand jury subpoena, or administrative order, disclose all information specified in the order and only that information.

3. If you are presented with a lawyer's subpoena or discovery request, ensure that the lawyer has either:
   - Informed the individual to whom the information applies of the proceeding sufficiently to allow them to agree or object, allowed enough time for the individual to agree or object, and resolved any objections the individual might have.
   - The lawyer obtained an authorization signed by the individual. (You may only disclose the information allowed by the authorization, not the subpoena)
   - Obtained a court order restricting the use of the information to the proceeding and requiring all parties to return or destroy the information when the proceeding is over (this is known as a "qualified protective order")

   If the lawyer has not done so, ensure that the privacy official at this organization has informed the individual and resolved any disputes, obtained an authorization or obtained a qualified protective order before disclosing any information. Disclose only that information described in the subpoena or discovery request or the authorization.

Actions To Be Taken When Disclosing Information In Facility Directories

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

2. Ensure that only the individual's name, location, general medical condition (stable, good, fair, poor) and religion are ever disclosed from the facility directory.

3. Disclose an individual's religious affiliation only to members of the clergy. You may disclose any other information described in step 1 above to members of the clergy as well, on request.

4. Disclose the location and general medical condition of individuals only to those persons (who are not members of the clergy) who ask for that individual by name.

Actions To Be Taken When Disclosing Information For Research, Marketing, Or Fundraising Purposes

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

2. Ensure that a valid Authorization has been obtained and filed before disclosing information for research, marketing or fundraising. Disclose only such information as allowed by the authorization.

3. If the organization's privacy board or review board has approved a waiver of authorization for research purposes, then that information may also be disclosed.

Actions To Be Taken When Disclosing Information To The Individual

This procedure is documented in the Procedures for Access Request section of this manual.

Actions To Be Taken When Disclosing Information To The Department Of Health and Human Services as Part Of A Compliance Review

This organization must cooperate fully with the Department of Health and Human Services (DHHS) when conducting compliance reviews. Answer all questions put to you by DHHS compliance investigators. Provide access to DHHS personnel to all requested records.

Actions To Be Taken When Disclosing Information About Deceased Individuals

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

2. Disclose information about deceased individuals to law enforcement only when they are suspected to be victims of a crime (or required to by court order or for purposes of identifying the perpetrator of a crime).

3. Disclose information about deceased individuals to medical examiners or funeral directors only as necessary to carry out their duties.

4. You may disclose information about the deceased to a coroner or medical examiner for the purpose of identifying the deceased, determining the cause of death, or other duties as allowed by your state laws.

5. You may disclose information about the deceased to funeral directors as necessary to carry out their duties. This information, if necessary, may be disclosed to the funeral director prior to, and in reasonable anticipation of, the individual's death. Prior to disclosing any information to a funeral director, the Privacy Official will check with state laws regarding such disclosures.

6. In all other cases, treat deceased individuals exactly as living individuals for purposes of information disclosures.

7. First, determine what the purpose is of the request for protected health information. If the request is made by a health care provider and purpose of the request is for *treatment purposes of a living family member only*, then you may share the deceased's protected health information with the health care provider of the living relative without an Authorization from their personal representative. If the purpose is for any other reason, then follow the next step.

8. Second, determine if the person requesting the deceased patient's protected health information is the deceased's *personal representative*. The Privacy Official will check with local state laws to determine who may act on the decedent's or the estate's behalf. Examples may include the legally authorized executor of the estate or the next of kin or other family member

9. If the person is the deceased's personal representative as allowed by state law, you must treat them as if they were the decedent. The personal representative may gain access to the deceased's protected health information, and may also sign an Authorization for you to disclose this information to another party.

Actions To Be Taken When Disclosing Information About Minors To Their Parents Or Guardians.

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

2. Determine if the parent or guardian is a personal representative. See the privacy official or the Personal Representative section of this manual to make that determination. If so, treat the parent or guardian as any other personal representative. If not, continue with the rest of this procedure.

3. Determine if state, local, case, or other applicable law requires that the information be disclosed to the parents or guardians. (See your privacy official, who may then consult an attorney) If so, disclose the information

4. Determine if state, local, case, or other applicable law explicitly permits the information to be disclosed to the parents or guardians. (See your privacy official, who may then consult an attorney) If so, disclose the information as necessary.

5. Determine if state, local, case, or other applicable law forbids the information to be disclosed to the parents or guardians. (See your privacy official, who may then consult an attorney) If so, do *not* disclose the information.

   If state, local, case, or other applicable law is completely silent on the issue, a licensed health care professional must make a professional judgment whether to allow, disclose, or forbid the information.

Information Requests

Actions To Be Taken For All Information Requests

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

2. Determine if your request for information is "routine" (carried out on an regular basis) or "non-routine" (special or unique requests)

3. Do *not* request an entire medical record unless an entire medical record is the minimum amount of information needed to accomplish your purpose.

Actions To Be Taken When Making Non-Routine Requests

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

2. Identify the purpose for which the request will be made. Be as specific as possible. (For example, you may suspect that some information that you maintain is incorrect and you want to "compare notes" with someone whom you believe has more up-to-date information.)

3. Identify the items of information required. Be as specific as possible. (For example, the results of a particular test performed on a particular day.)

4. For each item identified in the previous step, consider the effect of removing it from the request. That is, think about whether the purpose of the request would or would not be satisfied if the item were removed. If the item is not necessary for the purpose of the request, do not request the information. You may rely on the request being for the minimum amount of necessary information if it seems reasonable under the circumstances and the disclosure is to: a public official in the performance of his or her duties who states that the request is for the minimum information, the information is requested by another covered

entity, the request is from a professional member of the workforce or from a business associate and they state that the request is for the minimum information, or under an IRB or privacy board waiver of authorization for research.

5. Consider whether or not you should obtain an authorization from the individual to whom the requested information pertains.

Notice and Acknowledgement

Actions To Be Taken With Respect To Publication Of The Notice

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

2. Maintain the notice and update it when changes occur.

3. Maintain all versions of the notice in this organization's HIPAA Compliance file.

4. Also keep the notice behind the window for patients to review if asked for.

5. When the notice changes post the most current notice and replace the current notice given to patients with the revised notice as soon as possible and always within 30 days.

6. Keep 5 copies of the full notice available at all times.

7. Provide the notice to all established patients who have not previously been given the notice and all new patients after they check in for their first office visit.

8. Advise patients who need to receive the notice and sign an acknowledgement to arrive twenty minutes early for their scheduled appointment.

9. Ensure the notice is posted and maintained on this organization's website, in a prominent manner that is easy to find for anyone who might access the website.

Actions To Be Taken When Gaining Acknowledgement Of The Notice

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

2. Provide each patient receiving the notice with this organization's **Acknowledgement of Receipt of Notice of Privacy Practices**. The Acknowledgement is a separate page that is attached to every notice.

3. File the patient's signed acknowledgement in the patient's medical record under a separate tab.

4. If the patient refuses to sign the acknowledgement, contact the privacy official. The privacy official will answer any questions or concerns the patient may have.

5. *Never* condition treatment on refusal to sign the acknowledgement.

6. If the patient continues to refuse to sign the acknowledgement, document the efforts to explain the notice and subsequent failure to obtain a signature on the Acknowledgement form.

7. Patients 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 provide them with a notice and ask them to complete the acknowledgement.

8. The presentation of the notice is a time when a patient may request special privacy protections, alternate confidential communication channels, request to amend PHI, request a disclosure accounting, or request access to or copying of PHI. Forward all such requests to the privacy official.

Personal Representatives

Actions To Be Taken When Dealing With Personal Representatives

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

2. Recognize the circumstances when a personal representative relationship exists. These circumstances include:

    - If the person has the authority to act on behalf of the individual in making health care decisions. (See Karin Halstead if you have any questions. Karin Halstead will contact an attorney if necessary.)
    - The executor or administrator of a deceased person's estate is automatically a personal representative of the deceased individual.
    - A parent, guardian, or other person acting *in loco parentis* of an unemancipated minor is automatically a personal representative unless:
        - The minor consents, no other consent is required, and the minor has not requested that anyone be designated a personal representative.
        - The minor may lawfully obtain the treatment without parental consent and the minor, a court, or someone else who can lawfully consent to the treatment does so.
        - The parent assents to a confidentiality agreement between the minor and the health care provider.

3. Validate the personal representative relationship. If the nature of the relationship can be inferred from the circumstances (for example, when a parent brings a child in for treatment) you may treat such a person as a personal representative of the patient. Otherwise, obtain verification of the relationship between the two (such as a power of attorney

4. Restrict disclosures to personal representatives to those that are appropriate to the nature of the relationship between the personal representative and the patient. For example, a power of attorney may specify limitations on the representative's authority to act on the patient's behalf.

5. If the patient informs you that he or she wishes another individual to act in the capacity of a personal representative, HIPAA allows you to discuss the

patient's case with this third party as someone who is "involved in the patient's care," even though the third party may not be a "personal representative" in a legal sense. Disclosures to persons involved in the health care of others must be limited to those items that can be justified by the nature of the relationship.

Record Retention

Actions To Be Taken For Record Retention Purposes

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

2. Stamp the front cover of all files in this organization's HIPAA compliance file with an ink stamp titled "RETAIN FOR SIX YEARS" and the date.

3. ***Stamp any related record that is not filed in this organization's HIPAA compliance file with the above-mentioned stamps. Examples are:***
    - ***Records of disclosures that are subject to an accounting***
    - ***Authorizations***
    - ***Notices of privacy practices***

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

5. Starting on September 23, 2013, periodically review the files 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).

Regulatory Currency

Actions To Be Taken To Ensure Regulatory Currency

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

2. Install and review all new updates of the PrivaPlan HIPAA Privacy and Security Resource Kit within 30 days of receipt.

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

    - Newsletters and seminars provided by our professional liability carrier.
    - Regular review of the HIPAA Resources page of our state medical society as well as review of newsletters and email alerts from our medical society.

4. Within 30 days of becoming aware of a regulatory change, make changes to our policies, procedures and forms as appropriate to accommodate the regulatory changes.

5. Within 30 days of making the appropriate changes, train each member of the workforce who has a job function affected by the regulatory change.

Special Privacy Protection Request Processing

Actions To Be Taken For Special Privacy Protection Requests

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

2. Forward all requests for restriction of disclosures and uses of protected health information to Karin Halstead the Dr. Robert L. Ruxin's privacy official.

3. Contact all patients or their representatives who request restriction of their health information. Inform the patient or their personal representative that this practice requires the request be documented and submitted using our Request for Special Privacy Protections form. If the patient expresses concerns about completing the form invite them to visit so you can assist them in completing the form.

4. Track each request on the Request for Special Privacy Protections form.

5. Review the request form to verify the scope of restrictions and determine if these are uses or disclosures we are capable of restricting.

6. Document the grant or denial of restriction on the **Response to Request for Special Privacy Protections form** (which is incorporated into the Request for Special Privacy Protections form). Send a copy to the requestor.

7. If the request is granted, place one copy of the Request for Special Privacy Protections in the patient's electronic medical record under a separate tab. ***Add an alert to the notes section in the patient's chart to alert staff to the restriction***. Where appropriate a note will be made on the actual location of protected health information. File a second copy in this organization's HIPAA Compliance file.

8. If the request is granted, meet with the appropriate workforce members to ensure that the request is implemented in their operational activities.

9. Only act on requests that are documented in writing, by you or by the patient. Request that the patient complete a new Request for Special Privacy Protections for any new or additional requests.

10. Document any termination of restrictions on the original Request for Special Privacy Protections form. Fill out and send a copy of the Termination of Special Privacy Protection form (included in the Request of Special Privacy Protections form) to the patient if their request is terminated, in whole or in part. File a second copy in this organization's HIPAA Compliance file***. (This documentation must be retained for a period of six years past the date that it was last in effect.)***

Workforce Training and Awareness

Actions To Be Taken For Initially Training The Workforce

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

2. Complete and maintain an up-to-date listing of staff and their job descriptions. This will include independent contractors, 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.

3. Determine the policies and procedures for which each job description must be trained.

4. Create a training program using the Microsoft PowerPoint™ training materials found in the PrivaPlan Training folder, the HIPAA Ready Reference, PrivaPlan Stat, and the HIPAA Privacy Rule Training document, and if applicable use the PrivaPlan Multimedia HIPAA training tool.

5. Train each member of the staff in the topics which they must learn. Record each training session in the workforce training log; If you use the PrivaPlan Multimedia HIPAA training tool, modify the log procedure to incorporate use of the on line administrator's log of workforce training and certificates.

Actions To Be Taken For Training New Workforce Members

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

2. Give new staff as well as temporary staff a basic orientation in the policies and procedures related to their job function.

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

4. Ensure that all new management or new providers receive this training.

5. Ensure that new staff completes training within 30 days of their start date.

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

Actions To Be Taken For Ongoing Training Of The Workforce

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

2. Keep up to date a quick training reference guide using a) the Microsoft PowerPoint™ training materials in the Training folder, b) the **HIPAA Ready Reference** and c) PrivaPlan **Stat**.

3. Include a HIPAA awareness-training component in the 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 this practice's obligations.

4. Ensure that all existing staff understands this practice's computer, internet and email use policies and have signed to this effect.

5. At 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.

6. At 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. Additionally, the security official will remind staff about this organization's remote access policies and procedures.

7. Train each member of the workforce to not share their passwords or user ID's, to maintain a "strong" password (letters, numbers and symbols) and to change them according to this organization's procedure.

8. 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.

9. Train staff to use the security incident reporting forms whenever a suspected or actual security incident occurs. Train staff to recognize a security incident.

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

11. 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.

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

13. Maintain the workforce training log.

14. Review all patient privacy 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.

Sanctions

Actions To Be Taken For Initially Establishing HIPAA Sanctions

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. Karin Halstead 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 Karin Halstead BEFORE CONTINUING.

2. The privacy and security official has reviewed the HIPAA privacy and security procedures and policies of your organization. Determine the kinds of violations that might occur and prioritize by level of severity.

3. The privacy and security official has reviewed existing sanctions if any 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.

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

8. 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

Actions To Be Taken For Initially Establishing Business Associate Agreements

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

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

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

4. This organization has used business associate agreements that contain required HIPAA language and terms, including that necessary for HIPAA security.

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 and to be consistent with other aspects of the HIPAA requirements contained in the Business Associate Agreement.

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, in writing notify the business associate 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

6. Karin Halstead has been appointed as Dr. Robert L. Ruxin's "security official". The security official and Dr. Robert L. Ruxin will be responsible for completing the job description for the security official

7. The security official has met with Dr. Robert L. Ruxin to review the HIPAA Security rule and to determine the responsibilities of the security official.

8. Dr. Robert L. Ruxin has agreed to the following job description.

SECURITY OFFICIAL JOB DESCRIPTION

Security Official

Job-Sharing? No—this job is performed by the Practice Manager who is also the Privacy Official

Job Description:

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

Reporting structure:

The security official reports directly to the <insert name or job title>.

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 and existing 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. Ensure that all remote access to ePHI via portable devices, remote devices or workstations maintains these equivalent or better safeguards.
22. Ensure that all remote storage devices and their transport maintains these equivalents or better safeguards.
23. Manage the information systems activity review procedures and audit procedures.
24. Ensure ePHI integrity.
25. Ensure appropriate encryption or protection of any ePHI that is transmitted.

26. 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. Karin Halstead 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

3. The security official and senior management has determined that a [qualitative] [quantitative] [hybrid of the two] risk analysis will be performed.

4. The security official has followed and completed the steps outlined in the Risk Analysis PrivaGuide.

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

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

7. 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.

8. The security official will review the risk analysis and update if appropriate once each [six months]. The risk analysis will include both technical and non-technical safeguards.

9. 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.

10. As a routine risk management measure, the 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.

11. As a routine risk management measure, the security official will ensure the firewall is enabled on all workstations and enabled to the highest level of protection. 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.

12. As a routine risk management measure 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. Karin Halstead HAS REVIEWED THIS PROCEDURE.

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

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

4. If the security official determines there are infected 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 the security official will review the firewall security report to determine if there has been outside 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, the security official 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. Karin Halstead 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 Karin Halstead 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 Dr. Robert L. Ruxin 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. The security official 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.

5. 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 Dr. Robert L. Ruxin will not reassign the employee and will consult with appropriate counsel regarding employment practices for this employee.

6. 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.

7. 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.

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

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 password protection is in place on the PDA's or 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. Karin Halstead 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 Karin Halstead 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 the security official 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. The security official will disable the user account by calling the appreciate vendors, ie emr vendor, billing vendor etc. and have the account disabled.

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 backup 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 security official will immediately change the security alarm access code and notify all existing employees of the new access code.

6. 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.

7. 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.

8. 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.

9. 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. Karin Halstead HAS REVIEWED THIS PROCEDURE. IF, FOR ANY REASON, YOU CANNOT PERFORM EACH OF THESE STEPS AS DIRECTED, CONTACT Karin Halstead BEFORE CONTINUING.

2. 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 manage passwords.

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

4. The security official has met with Dr. Ruxin 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). [Note: Insert your "authentication" policy here. If you use tokens, pass phrases, biometrics or other systems describe those.]

8. The security official will ensure that all passwords are changed every 60 days.

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 all employees maintain the anti-virus software and security patches by NOT disabling the automatic update features and by running updates when alerted.

11. The security official, will determine if remote access is needed and if there is a valid business case for remote access or removing ePHI. The security official will ensure remote access devices (and storage media) have the same or equivalent password and related safeguards.

12. 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.

13. 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.

14. The security official will keep a written record of all passwords using the **Job Responsibilities with respect to PHI form**. This record will be kept in a locked area accessible only to the security official, privacy official, and [insert name of appropriate management]. In addition, a current copy is kept off-site in [insert an appropriate location, for example, a safe deposit box maintained by this organization].

15. 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.

16. 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.

Isolated Clearing House

This is done through our billing provider.

Malicious Software Protection

Actions To Be Taken To Develop and Maintain Malicious Software Procedures

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN Dr. Robert L. Ruxin 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 Karin Halstead BEFORE CONTINUING.

2. The security official has met with Dr. Ruxin to ensure their awareness and adherence to these procedures.

3. The security official has reviewed the **risk analysis** PrivaGuide 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 form** 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 [Insert additional as appropriate] 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 or other staff's personal laptop computers, PDAs and home computers [insert other appropriate 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, USB flash drives or other media that is

personal or 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 security official 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. Karin Halstead 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 Karin Halstead BEFORE CONTINUING.

2. The security official has met with Dr. Robert L. Ruxin 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, c) billing management 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 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 Karin Halstead 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 Karin Halstead BEFORE CONTINUING.

2. The security official has met with the Dr. Robert L. Ruxin 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 regulation governing identity theft and 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** (In the Document Templates folder) 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. The security official will remind staff and workforce members that there is no retaliation for reporting a security incident

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 Dr. Robert L. Ruxin 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.

14. The security official will update all procedures to ensure that security measures are enhanced to prohibit a future violation.

15. 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. Karin Halstead 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 Karin Halstead 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 backup 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. 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.

6. All backups are performed by our vendors (Athena Health for billing and EMR). Dr. Robert L. Ruxin and staff have no control over the procedure.

7. The security official will update the backup procedure to include new applications or data on both the incremental and weekly backup.

8. The security official will review the backup procedure with new users and ensure their data is stored on the server and included in the backup routine.

9. The security official 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. Karin Halstead 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 Karin Halstead BEFORE CONTINUING.

2. The security official will maintain a printed list of all companies 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 Dr. Robert L. Ruxin and the applicable staff who will be instructed to keep this print out always available.

3. The security official and Dr. Robert L. Ruxin have identified Athena Health as the emergency mode system.

4. In the event of a disaster or other situation requiring restoring data, the security official 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.

5. The security official will immediately locate the most current version of the data backup.

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

7. If the system or the office will not be accessible within 24 hours, the security officials will arrange for access to the physician's home computer which has been designated as the emergency mode "hot site" and restore the full system backup and then the most current incremental back up.

8. Vendors (Athena Health for billing and EMR) are responsible to all backup and restoration.

9. 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. Karin Halstead 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 Karin Halstead BEFORE CONTINUING.

2. The security official has met with the physician in charge 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 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 will review and re-conduct the risk analysis [every six months] to evaluate changes that could weaken the security measures in place.

7. The security official will also use the **PrivaPlan audit checklist** to 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. Karin Halstead 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 Karin Halstead BEFORE CONTINUING.

2. The security official has reviewed this procedure Dr. Robert L. Ruxin physician's in charge.

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. 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] in [offices] are kept secure 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, portable hard drives, 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. The security official will ensure that home computers that are used to access ePHI are kept physically secure at the home location. This will include training as well as assistance with appropriate safeguards or measures.

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

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

17. 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 structure checked after completion of repairs.

18. Alarm codes are changed whenever an employee is terminated.

19. 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.

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

21. Whenever hardware is relocated, and the hardware contains critical ePHI that is not already backed-up, an exact backup 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.

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

23. 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.

24. Whenever backup tapes, CD ROMs, floppy disks or hardware is re-used it will be completely cleaned of any ePHI using a commercially available software that erases all data.

Technical safeguards

Actions To Be Taken for Technical Safeguards and Access Controls

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

2. The security official has reviewed this procedure Dr. Robert L. Ruxin.

3. 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. The security official 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. 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.

6. Where applicable the security official will ensure that perimeter access (firewalls) require authentication by user ID, MAC address, or IP address. The security official will ensure that all firewalls or routers have password protection in place to protect their configuration from unauthorized persons.

7. The security official 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.

8. The security official 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.

9. Based on the ePHI inventory and risk analysis, the security official will ensure that a reasonably secure encryption methodology is activated on all system files maintained on the server, workstations, backup devices and their media and portable devices such as laptops. The security official will integrate state regulations governing breach of unencrypted computerized information to determine if the encryption should extend to personal data as well as ePHI. In the event the security official cannot ensure encryption, the reasons for this decision and alternate safeguards in place will be documented.

10. The security official will ensure that the email this practice uses for appointment scheduling and correspondence uses encryption software if and when ePHI is sent.

11. The security official will ensure that encryption is enabled on remote workstations like laptops or home based computers of any files, folders or applications where ePHI is created, maintained, stored or transmitted. This shall include storage devices like portable hard drives, back up tapes, USB flash drives and so forth. This will also include any MS Outlook folders on workstations if the Outlook data contains 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 has 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. If wireless access points are used for remote device access via home computer similar encryption and authentication will be enabled.

18. The security official will remind all workforce not to use public wireless access points that are unsecured unless their access is through the secure channels (VPN or SSL).

19. 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. 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 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 spyware software. Scans will review all system files and programs. Infected files will be quarantined and/or rebuilt.

21. 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.

22. 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 180 days.

23. Once every [two weeks] the security official 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.

24. 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.

Security Policies and Procedures

Actions To Be Taken for Implementing Security Policies and Procedures

1. FOLLOW THIS PROCEDURE EXACTLY AS IT IS WRITTEN. Karin Halstead 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 Karin Halstead BEFORE CONTINUING.

2. The security official has reviewed this procedure the physician in charge 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.