



HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT MODEL PRIVACY AND SECURITY POLICIES AND PROCEDURES

Revised July 2004

© 2002-2004 Illinois State Medical Society/ISMIE Mutual Insurance Company

**Reprinted with permission of the Illinois State Medical Society
and ISMIE Mutual Insurance Company**

Foreward

This document has been prepared by the Illinois State Medical Society (ISMS) and ISMIE Mutual Insurance Company to assist their members and policyholders in meeting the privacy and security requirements of the Health Insurance Portability and Accountability Act (HIPAA) passed by the Congress in 1996. It is used with permission of ISMS and ISMIE, and has been modified for South Dakota practitioners.

ISMS and ISMIE Mutual have attempted to compile all the basic information that physicians need to consider as they seek to comply with the HIPAA privacy and security requirements.

Does HIPAA Apply to You?

HIPAA applies to payors, institutions, health care professionals and providers, from the largest multi-state integrated delivery networks to solo practice professionals who engage in any of the “standard electronic transmissions.” Most physicians do at least some of their business electronically, so HIPAA applies to them. Many submit claims electronically, either directly from their offices or through a billing service. Others receive electronic payment and remittance information from health plans.

If your practice does any of the following electronically, either directly or through a billing service or other vendor, then HIPAA applies to you:

- submit claims;
- receive claim payment and remittance information;
- query insurance companies about the status of a claim;
- receive information about the status of a claim;
- query insurance companies about the eligibility of a patient to be covered for services;
- receive information about patient eligibility;
- send referral authorizations; or
- receive referral authorizations.

If your practice does not do any of the above electronically, either directly or through a billing service or other vendor, then HIPAA does not apply to you.

<p>NOTE: In order to bill Medicare after October 16, 2003, practices with 10 or more full time workforce members including the physicians must bill Medicare electronically and, as a result, will be subject to the HIPAA requirements.</p>

Document Organization

The document is divided into three general areas. The first deals with privacy policies and procedures, the second deals with security policies and procedures, and the third deals with administrative policies and procedures.

Each topic area begins with a background and is followed by a model policy and a procedure. Each model policy is a general statement about the way a practice might want to approach each topic area. Each model procedure provides specific examples of how the practice might want to implement that general policy.

Notes

NOTE: The model policies and procedures must be reviewed by each practice and modified as necessary. You must determine if and how these model policies and procedures apply to your practice, modify them so they do reflect your practice, and make any necessary changes to ensure your practice is in compliance with the HIPAA Privacy and Security Rules.

These model policies and procedures are intended primarily for small practices, as discussed below. If your practice is not a “small practice,” these model policies and procedures may in some cases not be appropriate for your practice, and should be modified appropriately. You should consult with your legal counsel if you have questions or concerns.

NOTE: These model policies and procedures are copyright by ISMS/ISMIE Mutual Insurance Co. Permission is granted to ISMS members and ISMIE Mutual Co. policyholders to use and modify these model policies and procedures so that they can bring their practices into compliance with HIPAA.

Permission also is granted to members of the South Dakota State Medical Association to use and modify these model policies and procedures so that they can bring their practices into compliance with HIPAA.

Other individuals and groups wishing to use or modify these model policies and procedures must seek written permission from ISMS/ISMIE Mutual Insurance Co. and pay a royalty to ISMS/ISMIE Mutual Insurance Co.

NOTE: This document does not constitute legal advice. You are urged to seek legal advice if you have any questions regarding how HIPAA applies to your practice.

Questions

If you have specific questions about HIPAA and your practice, contact your practice’s legal counsel.

Table of Contents

Organizational Overview	1
Privacy Policies and Procedures.....	2
Individual Rights	3
Individual Rights – Notice of Privacy Practices	3
Model Receipt of Notice of Privacy Practices Form.....	8
Model Consent for Release and Use of Confidential Information and Receipt of Notice of Privacy Practices Form	9
Individual Rights – Accounting for Disclosures of PHI.....	11
Disclosures of PHI Tracking Log	15
Requests for Accounting of Disclosures Log.....	16
Individual Rights – Inspect and Copy PHI	17
Inspection and Copying Request Log	21
Model Request for Medical Records Acceptance Form Letter	22
Model Request For Inspection or Copying of Confidential Information Denial Form Letter	23
Individual Rights – Request Amendment to PHI	24
Amendment Request Log.....	28
Model Acceptance of Request to Amend Medical or Billing Records Form Letter.....	29
Model Denial of Request to Amend Medical or Billing Records Form Letter	30
Individual Rights – Request Confidential Communications	31
Model Request for Confidential Communication	33
Request for Confidential Communications Log.....	34
Individual Rights – Request Restriction of Disclosures	35
Disclosure Restriction Log.....	37
Individual Rights – Authorizations.....	38
Model Authorization Form for Release of Confidential Health Information.....	42
Individual Rights – Waiver of Rights	44
Uses and Disclosures of Protected Health Information	45
Uses and Disclosures – Verification of Identity	45
Uses and Disclosures – Personal Representatives	48
Uses and Disclosures – Not Requiring Authorization	50
Uses and Disclosures – Do Not Apply to Practice	59
Uses and Disclosures – Minimum Necessary	61

Uses and Disclosures – Business Associates	64
Security Policies and Procedures.....	65
Administrative Safeguards	67
Administrative Safeguards – Risk Analysis, Risk Management and Ongoing Risk Evaluation.....	68
Administrative Safeguards – Contingency Planning	69
“PHI” Software Log.....	72
Backup Log.....	73
Administrative Safeguards – Physical Controls for Visitor Access	74
Physical Safeguards	75
Physical Safeguards – Access Control.....	76
Physical Safeguards – Records Processing – Receiving, Sending, and Disposing of PHI.....	81
Physical Safeguards – Computer Workstation Use and Security	86
Physical Safeguards – Device and Media Controls	88
Device and Media Controls Log	90
Technical Safeguards	91
Technical Safeguards – Personal or “Entity” Authentication.....	92
Technical Safeguards – Security Configuration – Documentation, Testing, Inventory, Virus Control.....	94
Technical Safeguards – Audit Controls and Integrity.....	96
Technical Safeguards – Transmission Security	97
Administrative Policies and Procedures	98
Administrative Requirements – Privacy Officer.....	98
Administrative Requirements – Security Officer	99
Administrative Requirements – Changes in Law	100
Administrative Requirements – Complaint Process	101
Complaint Log	103
Administrative Requirements – Information Access Management	104
Administrative Requirements – Mitigation of Privacy Breaches	105
Mitigation Log	106
Administrative Requirements – Security Incident Procedures	107
Security Incident Log.....	108

Administrative Requirements – Whistleblowers/Crime Victims	109
Administrative Requirements – Awareness and Training For Staff.....	111
Training Log	113
Model Acknowledgment of Training.....	114
Administrative Requirements – Workforce Sanctions	115
Administrative Requirements – Documentation.....	118
HIPAA Privacy and Security Readiness Checklist.....	121
Small Practice Security Risk Analysis	128
Appendices	135
Model Notice of Privacy Practices	135
Model Business Associate Agreement.....	139

Organizational Overview

Background

There are a variety of provisions in the Privacy Rule related to organizational requirements. In general, a covered entity – including a physician – must determine the type of organization in which they operate. For small practices, this is a fairly straightforward task. Small practices usually are not complex organizations.

Small practices:

- provide health care services;
- usually do not provide multiple covered functions;
- usually are owned by some or all of the physicians;
- are not business associates (see Uses and Disclosures – Business Associates, page 64);
- do not have “affiliates” (affiliates are separate legal entities with common ownership);
- are not “hybrid entities” (a hybrid entity is defined in a complex manner as “a single legal entity that is a covered entity and whose covered functions are not its primary functions”); and
- are not “organized health care arrangements” (separate covered entities that are integrated clinically or operationally are considered an organized health care arrangement if protected health information must be shared among the covered entities for the joint management and operations of the arrangement). **NOTE:** You may be an “organized health care arrangement” if you have a number of different independent physicians or other providers practicing in your office.

NOTE: Most physicians will be involved in an organized health care entity such as a hospital or ambulatory surgical treatment center. Physicians involved in such an entity should be aware of the entity’s HIPAA policies and procedures. The entity’s policies and procedures, not yours, will most likely apply when you provide services in those settings.

Privacy Policies and Procedures

Background

The Privacy Final Rule was issued December 28, 2000. The Privacy Final Rule was modified by the Privacy Modification Final Rule issued August 14, 2002. The Final Rule has subsequently been clarified through guidance issued by the government. All covered entities – including physician practices that engage in one of the standard HIPAA transactions, either directly or through a third party such as a billing service – are required to be in compliance with the rules.

This section of the document presents model privacy policies and procedures. ISMS and ISMIE Mutual developed these model policies and procedures to assist their members and policyholders, particularly small practices, with HIPAA Privacy Rule compliance. It is used with permission of ISMS and ISMIE, and has been modified for South Dakota practitioners.

Keep in mind that the Privacy Rule requires practices to keep confidential “protected health information” or PHI. For practical purposes and to ensure compliance with the Privacy Rule, in a small office, PHI is the same as confidential information, whether it is maintained in paper or electronic format, and includes all personal information such as name, address, and insurance information as well as medical information.

NOTE: The model policies and procedures must be reviewed by each practice and modified as necessary. You must determine if and how these model policies and procedures apply to your practice, modify them so they do reflect your practice, and make any necessary changes to ensure your practice is in compliance with the HIPAA Privacy Rules.

NOTE: These model policies and procedures are copyright by ISMS/ISMIE Mutual Insurance Co. Permission is granted to ISMS members and ISMIE Mutual Co. policyholders to use and modify these model policies and procedures so that they can bring their practices into compliance with HIPAA.

Permission also is granted to members of the South Dakota State Medical Association to use and modify these model policies and procedures so that they can bring their practices into compliance with HIPAA.

Other individuals and groups wishing to use or modify these model policies and procedures must seek written permission from ISMS/ISMIE Mutual Insurance Co. and pay a royalty to ISMS/ISMIE Mutual Insurance Co.

NOTE: This document does not constitute legal advice. You are urged to seek legal advice if you have any questions regarding how HIPAA applies to your practice.

Individual Rights

Individual Rights – Notice of Privacy Practices

Background

One section of the Privacy Rule addresses the Notice of Privacy Practices.¹ In general, a covered entity – including a physician – is required to provide every direct care patient with a copy of the covered entity’s Notice of Privacy Practices. In addition, covered entities are required to request and document the patient’s acknowledgment of receipt of the Notice, or document why the patient’s acknowledgment could not be received.

Model Policy

The practice provides a copy of its Notice of Privacy Practices to each direct care patient and documents that the Notice was provided. The practice makes its Notice available to other individuals upon request.

Model Procedure

Provision of Notice

The practice provides its Notice of Privacy Practices to every patient with whom it has a direct treatment relationship. The Notice is provided no later than the date of the first treatment to the patient after April 13, 2003.

Direct Treatment Relationship: As stated in the Privacy Rule, the practice has a direct treatment relationship with any patient with whom it does not have an indirect treatment relationship. An indirect treatment relationship is one where the practice delivers health care to the individual based on the orders of another health care provider and the practice typically provides services or products, or reports the diagnosis or results associated with the health care directly to another health care provider, who provides the services or products or reports to the individual. In general, if a provider never sees the patient in their office, the provider does not have a direct patient relationship.

NOTE: In a hospital, ambulatory surgical treatment center, or similar entity, the policies and procedures of the entity will apply when you provide services in such entities.

¹ § 164.520 – Notice of Privacy Practices for PHI.

The practice does not routinely have indirect treatment relationships with patients; however, in the case of an indirect treatment relationship, the practice makes its Notice available upon request to the patient in the indirect treatment relationship.

NOTE: Indirect treatment relationships include such relationships as a radiologist reading an X-ray ordered by another physician or a pathologist examining tissue.

NOTE: If your practice does routinely have indirect treatment relationships with patients, you will need to redraft and expand these procedures.

The practice makes its Notice available to any member of the public to enable prospective patients to evaluate the practice's privacy practices when making his or her decision regarding whether to seek treatment from the practice. The practice provides its Notice via e-mail to any patient or other individual who so requests the Notice.

NOTE: You must change this procedure if your practice will not provide your Notice via e-mail.

Documentation of Provision of Notice: When a direct treatment patient receives the Notice from the practice, the practice asks the patient to sign its "Receipt of Notice of Privacy Practices" form. (See the Model Receipt of Notice of Privacy Practices Form, page 8.) The form is filed with the patient's medical record. If the patient refuses to sign the form, it is noted in the medical record that the patient was given the Notice and refused to sign the form. Treatment is not affected by a refusal to sign.

NOTE: You may combine your Receipt of Notice of Privacy Practices with a consent to use and disclose PHI for treatment, payment, and health care operations. A Model Consent for Release and Use of Confidential Information and Receipt of Notice of Privacy Practices Form, page 9, has been included for this purpose. *ISMS and ISMIE Mutual recommend that physicians use this combined form.*

NOTE: A pediatric practice does not need to get a different acknowledgment for each child in a family. Rather, the practice can give the Notice to the guardian and ask the guardian to sign the acknowledgment for all of his or her children. The practice should place a copy of this acknowledgment in each of the children's medical records to document compliance.

Separate Document: The practice does not combine the Notice with any other documents.

Posting of Notice: The practice posts the Notice in a prominent place in its reception area and allows each patient to keep a copy of the Notice.

Electronic Notice: The practice does not routinely provide the Notice electronically. However, if the practice provides its first direct treatment service to a patient electronically, i.e., via e-mail, the practice delivers the Notice automatically and contemporaneously in response to the individual's first request for the service. A person who receives an electronic notice may still request a paper Notice.

NOTE: If the practice does provide the Notice electronically, then additional requirements apply.

- If the practice has a patient Web site, the practice must prominently post its Notice on the site and allow individuals to download the Notice.
- If the practice provides the Notice via e-mail:
 - the individual must agree to accept an electronic notice and that acceptance must be documented and not withdrawn by the individual;
 - if the practice knows the e-mail transmission has failed, the practice must provide a paper copy of the Notice to the individual.

Joint Notice: The practice is an independent practice; however, it is part of several organized health care arrangements with other covered entities, including the hospitals, nursing homes, ambulatory surgical centers, and other facilities at which its physicians practice.

NOTE: If you are a member of a group, the group is a single covered entity – a single practice – and the requirements for joint practice do not apply.

NOTE: If you are part of an organized health care arrangement, the arrangement – i.e., all covered entities in the arrangement – may have a joint notice which when signed by a patient at one covered entity applies to all of the covered entities in the arrangement. In this case, each covered entity must agree to abide by the terms of the joint notice and the notice must be expanded to indicate that the notice covers multiple entities and must reasonably describe the covered entities.

Notice Changes

If the Notice is revised, the practice makes the revised Notice available upon request beginning on the revision's effective date. The revised notice is posted in the practice's reception area and made available to all patients, including those who have received a previous Notice.

Content of the Notice

The Notice of Privacy Practices reflects and is based on the policies and procedures specified in this manual and referenced in this section.

NOTE: A model Notice of Privacy Practices is attached to these Model Policies and Procedures. See page 8.

Plain Language: The Notice is written in plain language. The practice strives for clarity. *[A sizeable proportion of the practice’s patients do not speak English and, as a result, the Notice also is made available in (list languages). OR Virtually all of the practice’s patients speak English, so the Notice is only made available in English.]*

Introductory Header: As required in § 164.520(b)(1)(i)), the first statement of the Notice states:

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

Statement of Uses and Disclosures: The Notice includes the following:

- a description, including at least one example, of the types of uses and disclosures that the practice is permitted to make under the Privacy Rule for treatment, payment, and health care operations;
- a description of each of the other purposes for which the Privacy Rule permits or requires the practice to use or disclose PHI without the individual's written authorization;
- a description of any material limitations or prohibitions imposed by the State or other applicable law on permitted uses and disclosures beyond that outlined in the first two bullet points;
- sufficient detail in each such description to place the individual on notice of the uses and disclosures that are permitted or required by the Privacy Rule and other applicable law; and
- a statement that other uses and disclosures will be made only with written authorization and that the individual may revoke such authorization.

In addition, the practice includes a statement that the practice may contact the individual with appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the individual.

Individual Rights: The Notice contains a description of the individual’s rights granted under the Privacy Rule:

- the right to receive confidential communications of PHI;
- the right to inspect, copy and request amendments to PHI; and
- the right to receive an accounting of PHI disclosures.

The practice allows individuals to request restrictions on the use and disclosure of PHI, but does not grant any of those requests.

The Notice states that the practice may not limit its obligation to make a use or disclosure of PHI that either the law requires or the Privacy Rule permits to prevent or lessen a serious and imminent threat to a person or public health or safety.

Duties of the Practice: The Notice outlines the practice's duties, including that the law requires the practice to:

- maintain the privacy of PHI and provide individuals with notice of the practice's legal duties and privacy practices with respect to PHI;
- abide by the terms of the Notice currently in effect; and
- include a statement that the practice reserves the right to change the terms of its Notice and to make the new Notice provisions effective for all PHI that it maintains. When this occurs, the practice provides individuals with a revised Notice at the patient's next visit or informs them of how to obtain a revised Notice.

Complaints: The Notice explains that individuals may complain to the practice's Privacy Officer and to the Secretary of the U.S. Department of Health and Human Services (HHS), if they believe their privacy rights have been violated. In addition, the Notice indicates how the individual may file a complaint and that the practice will not retaliate against any individual that files a complaint.

Contact: The Notice contains the title and telephone number of a person or office to contact for further information. That person is the practice's Privacy Officer.

Effective Date: The Notice contains an effective date, which is not earlier than the date on which the notice is published. The practice's initial notice was effective April 14, 2003.

Revisions to the Notice: The practice will promptly revise and provide its Notice whenever there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the Notice. Except when required by law, a material change to any term of the Notice will not be implemented prior to the effective date of the Notice in which such material change is reflected.

Documentation: The practice documents compliance with the Notice requirements by retaining a sample copy of each of its Notices of Privacy Practices. A signed copy or a copy indicating why an acknowledgment could not be received of the "Receipt of Notice of Privacy Practices" form is maintained in each patient's medical record. Copies of materials will be retained as required under section §164.630(j) for a period of six years from the date of creation or last use, whichever is later.

**Model Receipt of Notice of
Privacy Practices Form**

(ON OFFICE LETTERHEAD)

I, _____, hereby acknowledge receipt of the physician's Notice of
(Patient's Name)

Privacy Practices. The Notice of Privacy Practice provides detailed information about how the practice may use and disclose my confidential information.

I understand that the physician has reserved the right to change his or her privacy practices that are described in the Notice. I also understand that a copy of any Revised Notice will be provided to me or made available *[insert how it will be made available]*.

Signed: _____ Date: _____

If you are not the patient, please specify your relationship to the patient _____.

– Patient's file

Model Consent for Release and Use of Confidential Information and Receipt of Notice of Privacy Practices Form

(ON OFFICE LETTERHEAD)

I, _____, hereby give my consent to *[insert name of physician or practice]* to use or disclose, for the purpose of carrying out treatment, payment, or health care operations, all information contained in the patient record of _____.
(Name of Patient or Authorized Agent) (Patient's Name)

I acknowledge receipt of the physician's Notice of Privacy Practices. The Notice of Privacy Practice provides detailed information about how the practice may use and disclose my confidential information.

I understand that the physician has reserved a right to change his or her privacy practices that are described in the Notice. I also understand that a copy of any Revised Notice will be provided to me or made available *[insert how it will be made available]*.

I understand that this consent is valid until it is revoked by me. I understand that I may revoke this consent at any time by giving written notice to the physician of my desire to do so. I also understand that I will not be able to revoke this consent in cases where the physician has already relied on it to use or disclose my health information. Written revocation of consent must be sent to the physician's office.

Signed: _____ Date: _____

If you are not the patient, please specify your relationship to the patient _____.

– Patient's file

CONSENT FORM DEFINITIONS *[to be printed on reverse side of form]*

“Health care operations” refers to a large number of activities, including:

1. Conducting quality assessment and improvement activities, including outcome evaluation and development of clinical guidelines, provided that the obtaining of generalized knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
2. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;
3. Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance);
4. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
5. Business planning and development, such as conducting cost management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
6. Business management and general administrative activities including, but not limited to: (a) management activities relating to HIPAA privacy rule compliance; (b) customer services, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer; (c) resolution of internal grievances; (d) due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a covered entity or, following completion of the sale or transfer, will become a covered entity; and (e) creating de-identified health information, fundraising for the benefit of the covered entity, and marketing for which an individual authorization is not required.

“Payment” means the activities undertaken by the physician to obtain reimbursement for the provision of health care. These activities referred to in this definition relate to the individual to whom health care is provided and include, but are not limited to:

1. Determination of eligibility coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
2. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance, and related health care data processing;
3. Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
4. Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and
5. Disclosure to consumer reporting agencies of any of the following information relating to reimbursement: name and address, date of birth, Social Security number, payment history, account number, and name and address of the physician.

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

“Use” means the sharing, employment, application, utilization, examination, or analysis of patient information within the physician’s practice that maintains such information.

Individual Rights – Accounting for Disclosures of PHI

Background

Four sections of the Privacy Rule address tracking disclosures and the right of individuals to receive an accounting of disclosures.² In general, a covered entity – including a physician – is required to keep a history of when and to whom disclosures of protected health information (PHI) – confidential information – are made. Physicians *do not have to track* disclosures:

- for treatment, payment and health care operations – the most common reasons for disclosures;
- made to a patient or the patient’s representative;
- made as a result of a patient authorization;
- for the practice’s directory or to persons involved in the individual’s care;
- for national security or intelligence purposes;
- to correctional institutions or law enforcement officials with custody of the individual; and
- made prior to April 14, 2003.

All other disclosures must be tracked, including disclosures required by law such as mandated reports to public health agencies and information released as a result of a court order.

Model Policy

The practice tracks all disclosures of a patient’s protected health information (PHI) except disclosures (i) for the purposes of treatment, payment, and health care operations; (ii) that are made to the individual or to a person involved in the patient’s care; (iii) that are made as a result of a patient authorization; (iv) that are made for national security or intelligence purposes; or (v) to correctional institutions or law enforcement officials. Each patient is entitled to a copy of the list of disclosures of the patient’s PHI.

Model Procedure

Tracking Disclosures of Protected Health Information

Initial Date for Tracking Disclosures: The practice began accounting for disclosures of protected health information on April 14, 2003.

Exceptions to Accounting of Disclosures: The practice only tracks those disclosures required by the Privacy Rule. The practice does not track disclosures made:

² § 164.508 – Uses and Disclosures for which Authorization is Required; § 164.512 – Uses and Disclosures for Which Consent, an Opportunity to Agree or Object is Not Required; § 164.528 – Accounting of Disclosures of Protected Health Information; and § 164.530 (j) – Documentation Requirements.

- for treatment, payment or health care operations;
- prior to the effective date of the rule;
- made as a result of a patient authorization;
- to law officials or correctional institutions according to § 164.521(k);
- to the individual;
- for national security or intelligence purposes;
- to people involved in an individual's care; and
- for notification purposes as described in § 164.510.

The practice does track all other disclosures made as required by law, including public health reporting and disclosures mandated under worker's compensation laws.

Content of Information Tracked: The information tracked in relation to each disclosure is as follows:

- date of disclosure;
- name of covered entity or individual who received the information;
- description of information disclosed; and
- reason for disclosure.

This information is recorded on the Disclosures of PHI Tracking Log, page 15, and maintained by the Privacy Officer.

The practice also includes a copy of the Disclosures of PHI Tracking Log with the information about the patient's disclosure with the patient's medical record.

Requests for Accounting of Disclosures

Requests for Accounting of Disclosure: A request for an accounting for disclosures must be made in writing and mailed or sent to the practice. It should be marked "Attention: Privacy Officer."

Charge for Accounting of Disclosures: The practice allows an individual to request one accounting within a 12-month period free of charge. The practice charges a reasonable fee for more frequent accounting requests. The charge will be \$_____.

NOTE: If the practice does not intend to charge for multiple requests during a year, this procedure will need to be modified.

Disclosure Period Requested: An individual can request an accounting of disclosures for a period of up to six years prior to the date of the request. Requests for shorter accounting periods will be accepted. However, patients may only request an accounting of disclosures made on or after April 14, 2003.

Recording Requests for Accounting of Disclosures: The practice logs in all written requests on the Requests for Accounting of Disclosures Log, page 16. The log includes the date the request

was received, the name and address of the requestor, the date by which the practice must respond to the request, and the date the practice actually sent the response.

Response to Requests for Accounting of Disclosures: The practice responds to all requests for an accounting of disclosures within 60 days of receipt of the request. If the practice intends to provide the accounting for disclosures and cannot do so within 60 days, the practice informs the requestor of such and provides a reason for the delay and the date the request is expected to be fulfilled. Only one 30-day extension is permitted.

The right to receive an accounting of disclosures may be temporarily suspended by a law enforcement official or health oversight agency if the practice is notified by the law enforcement official or health oversight agency. The notice should indicate that law enforcement or agency efforts would be impeded if the accounting of disclosures was released. Typically, the notice is given to the practice in writing, but may be oral if the practice documents the notice. Oral notice can only be effective for 30 days. After 30 days, a written notice must be given.

NOTE: The practice should insist on a written notice not to disclose an accounting of disclosures meeting the following requirements: (1) be on law enforcement office stationary; (2) include the name and signature of the law enforcement official, including rank and telephone number; and (3) include the reason for non-disclosure.

Exceptions to Accounting of Disclosures: The practice only tracks those disclosures required by the Privacy Rule. The practice does not track, and cannot provide information related to, disclosures made:

- for treatment, payment or health care operations;
- prior to the effective date of the rule;
- to law officials or correctional institutions according to section § 164.521(k)(5);
- to the individual;
- made as a result of a patient authorization;
- for national security or intelligence purposes;
- to people involved in an individual's care; and
- for notification purposes as described in section § 164.510(b).

Content of Information Provided to Patient: The information provided in response to a request for disclosures includes the following for each disclosure:

- date of disclosure;
- name of covered entity or individual who received the information;
- description of information disclosed;
- reason for disclosure;
- copy of a written request for accounting; and
- date of last accounting request.

If a patient makes multiple requests, the practice only provides information since the last request.

A copy of any responses to a request for disclosures is filed with the patient's medical record.

Documentation

The practice documents disclosures and accountings of disclosures on the Disclosures of PHI Tracking Log and Requests for Accounting of Disclosures Log. This information, along with the requests for disclosures, the responses of the practice, and any related correspondence, is retained as required under section § 164.630(j) for a period of six years from the date of its creation.

Individual Rights – Inspect and Copy PHI

Background

One section of the Privacy Rule addresses the right of individuals to inspect and copy PHI.³ In general, a covered entity – including a physician – is required to allow an individual access to inspect and obtain a copy of protected health information (PHI) about the individual for as long as the information is maintained. The information must be maintained in a “designated record set.” This right does not extend to:

- psychotherapy notes;
- information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and
- information maintained by a covered entity that is subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. 263a, to the extent the provision of access to the individual would be prohibited by law, or exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR 493.3(a)(2).

A covered entity may also deny access for several specific reasons listed in the Privacy Rule (see below).

Model Policy

The practice allows individuals to inspect and copy their protected health information (PHI), documents all requests, responds to those requests in a timely fashion, informs individuals of their appeal rights when a request is rejected in whole or in part, and charges a fee equal to the actual cost of copying and mailing of the records.

NOTE: Practices often receive PHI from outside sources, e.g., medical records from other practices, lab reports, and x-rays. This so-called “secondary record” PHI is incorporated into the practice’s medical records. As such, it becomes part of the practice’s medical records and is not treated differently from the PHI created by the practice. Accordingly, *PHI from outside sources is available for inspection and copying, regardless of source, in the same manner as the rest of the medical record.*

³ § 164.524 – Access of Individuals to Protected Health Information.

NOTE: South Dakota law imposes a misdemeanor criminal penalty for failure to disclose a patient's medical record to the patient or the patient's designee upon written authorization from the patient. SDCL 36-2-16. The HIPAA privacy rules allow the practitioner to refuse to disclose information in some circumstances. See, e.g., 45 CFR 164.524. If you are in doubt concerning whether you should or must allow an individual to inspect or copy some or all of his protected health information (PHI), you should consult with your practice's legal counsel.

Model Procedure

Submission of Requests for Inspection and Copying of PHI: Requests for the inspection and copying of records must be sent to the practice in writing. They must be sent to the attention of the practice's Privacy Officer.

Receipt of Request: Upon receipt of a request, the practice records the request on the Inspection and Copying Request Log, page 21. The log includes, among other things, the date of receipt, the name of the requestor, and the information requested. The Privacy Officer maintains the request with the log.

Review of Request: The practice reviews the request in a timely fashion and acts on a request for access generally within 30 days. The practice may have a single extension of 30 days, if needed to act on the request.

Each request will be accepted or denied and the requestor notified in writing. If a request is denied, the requestor is informed whether the denial is "reviewable" or not. In any case, the requestor is informed of how to appeal any denial.

NOTE: South Dakota law imposes a misdemeanor criminal penalty for failure to disclose a patient's medical record to the patient or the patient's designee upon written authorization from the patient. SDCL 36-2-16. The HIPAA privacy rules allow the practitioner to refuse to disclose information in some circumstances. See, e.g., 45 CFR 164.524. If you are in doubt concerning whether you should or must allow an individual to inspect or copy some or all of his protected health information (PHI), you should consult with your practice's legal counsel.

Unreviewable Grounds for Denial: The practice denies a requestor access to PHI without the opportunity to appeal the decision in the following cases:

- requests for psychotherapy notes;
- information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding;
- information maintained by the practice that is subject to the Clinical Laboratory exemptions, as provided by the Privacy Rule;
- treatment information created or obtained in the course of research may be temporarily suspended for as long as the research is in progress;

- records that are subject to the Privacy Act, 5 U.S.C. § 552a [records held by the federal government], access may be denied, if the denial of access would meet the requirements of that Act; and
- if the information was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

If a request falls into one of these categories, the practice will deny the request.

Reviewable Grounds for Denial: When the practice denies access to inspect and copy for any of the following reasons, the requestor is allowed to appeal the decision:

- the practice has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
- the information makes reference to another person (who is not a health care provider) and the practice has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or
- the request for access is made by the individual's personal representative and the practice has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

If a request falls into one of these categories, the practice will deny the request and inform the requestor of their right to appeal the decision.

Notification of Denial: If the practice denies access, in whole or in part, to requested information, the practice:

- makes information not denied accessible;
- provides a timely, written denial to the individual in plain language that contains:
 - the reason for the denial;
 - if applicable, a statement of the individual's right to review;
 - a description of how the individual may complain to the practice or to the Secretary, including the telephone number of the practice's Privacy Officer; and
 - if the practice does not maintain the information requested, and the practice knows where the information is maintained, a description of where to direct the request for access.

See Model Request For Inspection or Copying of Confidential Information Denial Form Letter, page 23.

The Privacy Officer maintains the notification with the Inspection and Copying Request Log.

Review of Denial of Access: The practice's Privacy Officer determines, within a reasonable period of time, whether or not to grant the access. A reasonable time period for review of records is no more than 30 days. Further, the practice allows an individual to appeal a

“reviewable” denial. The requestor has the right to have the denial reviewed by a licensed health care professional who is designated by the practice as a reviewing official and who did not participate in the original decision to deny. The practice informs the requestor of the decision of the reviewing official and adheres to the decision.

Charging for Request: The practice charges a fee equal to the actual cost of copying and mailing, as applicable. The practice will determine the charge for providing the requested records and inform the requestor in advance of providing the records. If the requestor agrees to pay the fee in advance, the records will be provided. Otherwise, the records will not be provided, unless the Privacy Officer determines that the charge is burdensome to the requestor.

Documentation

In accordance with § 164.524(e) the practice allows an individual to inspect and copy all information in the designated record set, except as otherwise provided above. The designated record sets include:

- the patient’s medical record; and
- the patient’s billing record.

The practice will document requests for inspection and copying of PHI on the Inspection and Copying Request Log. This information, along with the request of the PHI, the response from the practice, and any related correspondence, will be retained as required under section §164.630(j) for a period of six years from the date of its creation.

NOTE: The practice is required to maintain the documentation for 6 years. This requirement may in some circumstances change the record retention periods for medical records under South Dakota law. See SDCL 36-4-37 and 36-4-38.

Model Request for Medical Records
Acceptance Form Letter

(ON OFFICE LETTERHEAD)

Date: _____

Dear *(Patient or Representative)*:

Attached are copies of the requested medical records for _____ *(patient's name)* _____.

Medical records consistent with your request have been provided. If this office is in possession of other records or information that, by statute or regulation, require special authorization from the patient to release, and no specific release has been received, these records or information have not been provided.

Also enclosed is an invoice for the cost of reproducing these records and mailing them to you. Please send payment to the above address.

Sincerely,

cc: Patient's file
Attached records
Enclosed invoice

Model Request For Inspection or Copying of Confidential Information Denial Form Letter

NOTE: South Dakota law imposes a misdemeanor criminal penalty for failure to disclose a patient's medical record to the patient or the patient's designee upon written authorization from the patient. See SDCL 36-2-16. The HIPAA privacy rules allow the practitioner to refuse to disclose information in some circumstances. See, e.g., 45 CFR 164.524. If you are in doubt concerning whether you should or must allow an individual to inspect or copy some or all of his protected health information (PHI), you should consult with your practice's legal counsel.

(ON OFFICE LETTERHEAD)

Date: _____

Dear *(Patient or Representative)*:

Your request for inspection or copying of your medical record is denied because _____

(Reason for denial)

This request may be appealed ____ Yes ____ No.

[If applicable: You have requested records that we do not possess. We suggest you attempt to obtain the record from _____].

If applicable, you may appeal this decision by written complaint to:

(Practice designated reviewer – Probably Privacy Officer)

In addition, you may also file a complaint with or appeal this decision to the Secretary, U.S. Department of Health and Human Services: Office for Civil Rights, U.S. Department of Health & Human Services, 1961 Stout Street - Room 1426 , Denver, CO 80294, Phone - (303) 844-2024; TDD - (303) 844-3439, Telefax - (303) 844-2025

Sincerely,

cc: Patient's file
Privacy Officer

Individual Rights – Request Amendment to PHI

Background

Two sections of the Privacy Rule address the right of individuals to request an amendment to PHI.⁴ In general, a covered entity – including a physician – is required to amend PHI or a record about the individual in a “designated record set” for as long as the PHI is maintained in the “designated record set.”

A covered entity may deny a request for amendment if:

- the information was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;
- the amendment relates to information that is not part of the designated record set;
- the information would not be available for inspection (see Individual Rights – Inspect and Copy PHI, page 17); or
- the information is accurate and complete.

Model Policy

The practice allows an individual to request that the practice amend the protected health information (PHI) maintained in the patient’s medical record or the patient’s billing record – the practice’s designated record set. The practice documents all requests, responds to those requests in a timely fashion, and informs individuals of their appeal rights when a request is denied in whole or in part.

Model Procedure

Written requests: The practice accepts requests to amend the PHI maintained by the practice. The requests must be in writing and must be sent to the practice’s Privacy Officer.

Designated Record Set: The practice considers its patients’ medical records and patients’ billing records to be its designated record set.

Receipt of Request: Upon receipt of a request, the practice records the request on the Amendment Request Log, page 28, and maintains the request with the log. The log includes, among other things, the date of receipt, the name of the requestor, and the amendment requested. A copy also is kept with the patient’s medical record.

Timely Action: The practice will act on a request for amendment no later than 60 days after receipt of such a request, as follows:

⁴ § 164.526 – Amendment of Protected Health Information; and § 164.524(a)(2)&(3) – Unreviewable and Reviewable Grounds for Denial.

- If the practice accepts the amendment, in whole or in part, the practice takes the actions set forth below.
- If the practice denies the amendment, in whole or in part, the practice provides the requestor with a written denial as described below.
- If the practice cannot act on the amendment within 60 days, the practice extends the time for such action by 30 days and, within the 60-day time limit, provides the requestor with a written statement of the reasons for the delay and the date by which the practice will complete action on the request. Only one such extension is allowed.

Acceptance of Requests: If the practice accepts the request, in whole or in part, the practice:

- makes the requested amendment to the PHI by, at a minimum, identifying the portion of the medical record or billing record being amended and inserting the amendment into the record. *The practice will not, under any circumstances, delete or destroy any portion of the medical record. The practice will simply amend the medical record by the addition of notes;*
- informs the requestor that the amendment has been accepted and obtains the requestor's identification of and agreement to have the practice notify other relevant parties of the amendment;
- makes reasonable efforts to inform and provide the amendment within a reasonable time period to relevant parties identified by the requestor and to other parties, including business associates, that the practice knows the PHI is being amended.

(See the Model Acceptance of Request to Amend Medical or Billing Records Form Letter, page 29, and the Model Denial of Request to Amend Medical or Billing Records Form Letter, page 30.)

Denial of Requests: If the practice denies the request, in whole or in part, the practice provides the requestor with a written denial in a timely fashion (as detailed above). The denial is written in plain language and includes:

- the basis for the denial;
- the requestor's right to submit a written statement disagreeing with the denial and that the requestor may file such a written statement with the practice addressed to the attention of the practice's Privacy Officer;
- a statement that, if the requestor does not submit a statement of disagreement, the requestor may request that the practice provide a copy of the request for amendment and the denial with any future disclosures of the PHI that is the subject of the request; and
- a description of how the requestor may complain to the practice or to the Secretary, including that the complaint should be addressed to the practice's Privacy Officer at the practice's telephone number.

The practice may deny a request if:

- the information was not created by the practice, unless the requestor provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;
- the amendment relates to information that is not part of the designated record set;
- the information would not be available for inspection (see Individual Rights – Inspect and Copy PHI, page 17); or
- the information is accurate and complete.

Disagreement by the Requestor: The practice allows a requestor to submit a written statement disagreeing with the denial of all, or part, of the initial request. The statement must include the basis of the disagreement. The practice limits the length of a statement of disagreement to one page.

Practice Rebuttal Statement: The practice may prepare a written rebuttal to the requestor's written disagreement. When a rebuttal statement is prepared, a copy will be sent to the requestor.

Future Disclosures: If a request for amendment has been denied by the practice, future disclosures are subject to the following requests:

- if a written statement of disagreement has been submitted by the requestor, the practice includes a copy of the initial request, the denial of the request, the disagreement with the denial, and any rebuttal of the disagreement or, at the election of the practice, an accurate summary of any such information, with any subsequent disclosure of the PHI to which the disagreement relates; or
- if the requestor has not submitted a written statement of disagreement, the practice includes the initial request and the denial of the request, or an accurate summary of such information, with any subsequent disclosure of the PHI to which the disagreement relates, if the requestor has requested such release.

If a subsequent disclosure is made of the PHI, which is the subject of the disagreement using a standard electronic transaction under Part 162 of the HIPAA rule, and that disclosure does not permit the additional material to be included with the transaction, the practice separately transmits the material required to the recipient of the standard transaction.

Notification of Amendment by Another Entity: If the practice is notified that another covered entity has amended PHI maintained by the practice, the practice must also amend the PHI in its possession.

Documentation

In accordance with § 164.526(f), the practice designates the Privacy Officer as the individual responsible for receiving and processing requests for amendments. In addition, the practice will retain the documentation as required by § 164.530(j), including the information included in the Amendment Request Log, the request for amendment, the response of the practice to the

amendment, and any other related correspondence with the requestor. This information will be maintained for a period of six years from the date of its creation.

NOTE: This requirement may in some circumstances change the record retention periods for medical records under South Dakota law. See SDCL 36-4-37 and 36-4-38.

**Model Acceptance of Request to Amend
Medical or Billing Records Form Letter**

(ON OFFICE LETTERHEAD)

Date: _____

Dear (*Patient or Representative*):

Your request to amend your medical or billing records has been accepted and will become part of your medical or billing record.

Please let the practice know within 30 days what, if any, other health care providers, health care professionals or health plans should receive a copy of this amendment.

The cost of copying and mailing for each such provider, professional or plan is \$____. Please send payment to the above address for any copies you would like sent.

Sincerely,

cc: Patient's file
Privacy Officer

**Model Denial of Request to Amend
Medical or Billing Records Form Letter**

(ON OFFICE LETTERHEAD)

Date: _____

Dear *(Patient or Representative)*:

Your request to amend your medical or billing record is denied because _____

(Reason for denial)

You may submit a written one-sided 8½” x 11” page statement disagreeing with the denial of your request to amend to the practice Privacy Officer within 30 days of receipt of this denial. Please note: The practice may prepare a rebuttal statement. If no statement is submitted, you may request that a copy of the requested amended record and denial be included when your medical or billing records are disclosed.

Any correspondence must be sent to:

(Practice designated reviewer – Probably Privacy Officer)

In addition, you may file a complaint with the Secretary, Office for Civil Rights, U.S. Department of Health & Human Services, 1961 Stout Street - Room 1426 , Denver, CO 80294, Phone - (303) 844-2024; TDD - (303) 844-3439, Telefax - (303) 844-2025

Sincerely,

cc: Patient’s file
Privacy Officer

Individual Rights – Request Confidential Communications

Background

Two sections of the Privacy Rule address the right of an individual to request that certain communications be kept confidential.⁵ In general, a covered entity – including a physician – is required to accommodate all reasonable requests to keep communications confidential.

Model Policy

The practice accommodates all reasonable requests to keep communications confidential. The practice determines reasonableness based on the administrative difficulty of complying with the request.

Model Procedure

Request for Confidential Communications: A request for confidential communications must be in writing, must specify an alternative address or other method of contact, and must provide information about how payment will be handled. The request must be on the **Model Request for Confidential Communication**, page 33, and addressed to the practice’s Privacy Officer. No reason for the request needs to be stated. The request will be recorded on and maintained with the Request for Confidential Communications Log, page 34.

Determination of Reasonableness of Request: The practice accommodates all reasonable requests. The reasonableness of a request is determined solely on the basis of the administrative difficulty of complying with the request.

The practice will reject a request due to administrative difficulty:

- if no independently verifiable method of communication, such as a mailing address or published telephone number, is provided for communications, including billing; or
- if the requestor has not provided information as to how payment for services will be handled.

The practice will not refuse a request:

- if the requestor indicates that the communication will cause endangerment; or
- based on any perception of the merits of the requestor’s request.

⁵ § 164.522(b) – Rights to Request Privacy Protection for Protected Health Information – Standard – Confidential Communications Requirements; and § 164.502(h) – Uses and Disclosures of Protected Health Information – General Rules – Standard – Confidential Communications.

In any case, clear methods of communication with the requestor should exist.

If a request is accepted, the practice will include a copy of the acceptance with the patient's medical record to ensure the agreed confidential communication occurs.

Documentation

In accordance with §164.526(f), the practice designates the Privacy Officer as the individual responsible for receiving and processing requests for confidential communications. In addition, the practice retains the documentation as required by §164.530(j), including the Request for Confidential Communications Log, the written request for confidential communications and the practice's response to that request. This information will be maintained for a period of six years from the date of its creation.

NOTE: This requirement may in some circumstances change the record retention periods for medical records under South Dakota law. See SDCL 36-4-37 and 36-4-38.

Model Request for Confidential Communication

I, _____, hereby request *[insert name of physician or practice]*
(Name of Patient or Authorized Agent)

to keep communications regarding my protected health information confidential. To accomplish this goal, please do the following:

Phone: You can contact me by phone at _____

Leave messages on answering machine: ___ Yes ___ No

Leave message with any other person: ___ Yes ___ No

Mail: Contact me at the following address: _____

FAX: ___ Please do not contact me by FAX

___ Please contact me by FAX at _____

Other Requests for Confidential Communications: _____

This request may be changed or revoked by filing a new request or revoking this one in writing.

Signed: _____ Date: _____

If you are not the patient, please specify your relationship to the patient: _____

– Patient’s file

Individual Rights – Request Restriction of Disclosures

Background

One section of the Privacy Rule addresses the right of individuals to request a restriction on disclosures.⁶ In general, a covered entity – including a physician – is required to have a policy with respect to allowing individuals to request restrictions on the use and disclosure of their PHI. A covered entity is not required to agree to any restriction.

Model Policy

The practice accepts all requests for restrictions of disclosures of protected health information (PHI). The practice does not agree to any restrictions in the use or disclosure of PHI.

Model Procedure

All requests for restrictions of disclosures must be submitted in writing. They must be sent to the attention of the practice's Privacy Officer. Each request is recorded on and maintained with the Disclosure Restriction Log, page 37. The Privacy Officer notifies the requestor in writing that the practice does not accept restrictions on disclosure and notes on the Disclosure Restriction Log the date the written notification was provided.

Documentation

The practice retains the documentation as required by § 164.530(j), including the Disclosure Restriction Log, the written request for restriction, and the practice's response to that request. This information is maintained for a period of six years from the date of its creation.

NOTE: A practice could agree to restrictions. In this case, the practice will have to document and track each restriction, and will have to ensure that it adheres to each restriction. To simplify practice operations, practices should consider not agreeing to any restriction on the use or disclosure of PHI.

Keep in mind that if a practice agrees to restrictions:

- It may not use or disclose PHI in violation of the restriction except in situations when the individual who requested the restriction is in need of emergency treatment and the restricted information is needed to provide the treatment, and must develop procedures to ensure that information is not disclosed in violation of an agreed restriction.
- It may terminate its agreement to a restriction. The individual or the practice can initiate the termination and the termination is only effective

⁶ § 164.522(a) – Rights to Request Privacy Protection for Protected Health Information – Standard – Right of an Individual to Request Restriction of Uses and Disclosures.

with respect to PHI created or received after the practice has informed the individual of the termination. Information created or received prior to lifting the restriction may be released by agreement. The practice must develop procedures to ensure that information covered while the restriction was in effect is not disclosed in violation of the agreed restriction.

- It must document the restriction and maintain that documentation for a period of 6 years.

NOTE: These requirements may in some circumstances change the record retention periods for medical records under South Dakota law. See SDCL 36-4-37 and 36-4-38.

Disclosure Restriction Log

Patient Name	Request Date	Description of Request	Response Denied	Date Response Sent
			X	
			X	
			X	
			X	
			X	
			X	
			X	
			X	
			X	
			X	
			X	
			X	
			X	
			X	

Individual Rights – Authorizations

Background

Nine sections of the Privacy Rule address patient authorizations.⁷ In general, a covered entity – including a physician – is required to obtain an authorization for the use or release of information for other than treatment, payment, or health care operations, unless state or federal law requires such disclosure.

Model Policy

The practice obtains a written authorization from a patient or the patient’s representative for the use or disclosure of protected health information (PHI) for other than treatment, payment, or health care operations. However, the practice will not require an authorization for the use or disclosure of PHI specifically allowed under the Privacy Rule in the absence of an authorization, except for PHI requiring an authorization under South Dakota law. Such uses and disclosures are discussed under “Uses and Disclosures – Not Requiring Authorization” beginning on page 50.

NOTE: There is no requirement for physicians to develop authorizations; however, physicians may want to do so in some instances as a service to patients. For example, a parent may ask a physician to send certain confidential information about their child to a camp or school. The physician has two options. First, the physician can provide the information directly to the parent and allow them to release it to the camp or school. Second, the physician can use an authorization form to allow them to send the information directly to the camp or school. Keep in mind that this latter approach may be burdensome on practices. Each authorization has to be specific to the release under consideration.

NOTE: Automobile insurance, homeowners insurance, and similar policies (other than the patient’s own health care insurance policy) that provide coverage for health care expenditures in most circumstances are not considered a “health plan” under HIPAA, and therefore a signed authorization is required prior to releasing PHI to such entities.

NOTE: The HIPAA Privacy Rules do not apply to disclosures for purposes related to claims for workers’ compensation benefits, except that only the minimum necessary to comply with the workers’ compensation-related request is to be provided absent an authorization. However, a signed authorization usually

⁷ § 164.506(a) – Standards for Consents and How Consents Differ from Authorizations; § 164.508(a) – Standard for Requirements and Exceptions for Authorizations; § 164.508(b) – Implementation Specifications for Authorizations; § 164.508(c) – Core elements and requirements; § 164.508(d) – Specifications for an Entity’s Own Uses and Disclosure; § 164.508(e) – Specifications for an Entity’s Disclosure to Others; § 164.508(f) – Specifications for Research and Treatment; § 164.520 – Requirements for Plain English Language; and § 164.512 – Uses and Disclosures for which Consent, an Authorization, or Opportunity to Agree or Object is *Not* Required.

is not required for release of PHI for worker's compensation claims. This is because such release of PHI is required by law (see Uses and Disclosures Required by Law, page 51). (See also, SDCL 62-4-45)

Model Procedure

Situations in which the practice does not obtain the individual's authorization to use or disclose PHI are discussed under "Uses and Disclosures – Not Requiring Authorization" beginning on page 50.

Elements of an Authorization: Every authorization used by the practice includes the following core elements:

- the name of the practice;
- a description of the information to be used or disclosed by the practice;
- the name of the recipient(s) or class of recipient of the use or disclosure;
- an expiration date, time period or event following which the authorization terminates;
- a statement regarding the individual's right to revoke the authorization and a description of how the individual may revoke the authorization;
- a statement that the information may be subject to re-disclosure by the recipient and may no longer be protected by the federal privacy law;
- the individual's signature and date of signature; and
- if signed by a representative, a description of the representative's authority to act for the individual and/or relationship to the individual.

In addition to the core elements, when the authorization is for the practice to use or disclose the information for its own purposes, the authorization also includes:

- a statement that the practice does not condition treatment on the provision of the authorization for the requested use or disclosure;
- a description of the purpose of the requested use or disclosure;
- the right of the individual to inspect or copy the PHI to be used or disclosed;
- the right of the individual to refuse to sign the authorization; and
- a statement of any remuneration direct or indirect that the practice will receive from a third party as a result of the disclosure.

In addition to the core elements, when the authorization is for the practice to disclose information to others, the authorization also includes:

- a description of each purpose of the requested disclosure (the statement "at the request of the individual" is sufficient description of the purpose when an individual initiates the authorization and does not or elects not to provide a statement of purpose);
- a statement that the practice does not condition treatment on the provision of authorization for the requested use or disclosure; and
- a statement that the individual may refuse to sign the authorization.

Authorizations for Research: The practice does not participate in research and, accordingly, does not have any authorizations related to research studies.

NOTE: A practice may want to participate in research and provide PHI as part of that research. In that instance, this policy must be changed. Research is a complex area and most small practices do not engage in research. (See Research Activities, page 59.)

Conditioning Care on Authorization: The practice does not condition treatment of a patient on the signing of an authorization, except:

- disclosure necessary to determine payment of claim (excluding authorization for use or disclosure of psychotherapy notes); or
- provision of health care solely for purpose of creating PHI for disclosure to a third party (e.g., drug screening, fitness-for-duty examinations, pre-employment or life insurance physicals).

Compound Authorizations: The practice does not combine an authorization for use or disclosure of PHI with any other document, except:

- an authorization for a use or disclosure of psychotherapy notes may be combined with another authorization for a use or disclosure of psychotherapy notes; and
- an authorization, other than for psychotherapy notes, may be combined with another authorization, except when the practice has conditioned the provision of treatment on the execution of one of the authorizations.

NOTE: A practice that does not keep any psychotherapy notes may eliminate the first exception as it is unnecessary.

Revocation of Authorizations: The practice allows an individual to revoke an authorization at any time. The revocation must be in writing and must be sent to the attention of the practice's Privacy Officer; however, the practice will be able to use or disclose the PHI to the extent that the practice has already taken action in reliance on the authorization.

Defective Authorizations: The practice recognizes that an authorization is defective or invalid if:

- the expiration date or event has passed;
- the authorization is not filled out completely;
- the authorization is revoked;
- the authorization lacks a required element; or
- the authorization violates requirements regarding compound authorizations.

Copy to Patients: The practice will provide a patient, upon request, a copy of any authorization initiated by the practice (as opposed to requested by the patient) and signed by the patient.

Psychotherapy Notes: Psychotherapy notes are defined as follows:

notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

The practice requires an authorization for use and disclosure of psychotherapy notes except for the following uses:

- use by the originator of the psychotherapy notes for treatment;
- use or disclosure by the practice in training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; and
- use or disclosure by the practice to defend a legal action or other proceeding brought by the individual.

NOTE: A practice that does not keep any psychotherapy notes may eliminate these exceptions as they are unnecessary.

Documentation

The practice will retain copies of all authorizations and revocations of authorizations for a period of six years from the date of its creation.

NOTE: This requirement may in some circumstances change the record retention periods for medical records under South Dakota law. See SDCL 36-4-37 and 36-4-38.

Model Authorization Form for Release of Confidential Health Information

(ON OFFICE LETTERHEAD)

I, _____, hereby authorize insert name of physician to release to:
(Name of Patient or Authorized Agent)

(Name of Health Care Facility, Physician, Agency, etc.)

(Street Address, City, State and Zip Code)

the following information contained in the patient record of _____
(Patient's Name)

born _____, residing at _____:
(Birthdate) (Street Address, City, State and Zip Code)

- The entire medical record, **excluding** mental health treatment, alcoholism treatment, drug abuse treatment, and HIV/acquired immune deficiency syndrome (AIDS) records

To be disclosed, the following items must specifically be checked:

- Mental Health Treatment Records
- Alcoholism Treatment Records
- Drug Abuse Treatment Records
- Genetic Testing
- HIV/Acquired Immune Deficiency Syndrome (AIDS) Records
- Laboratory Reports
- X-ray Reports
- Other: _____

The above information for the following period of time shall be released:

From: _____ to _____.
(Date) (Date)

The purpose(s) of the authorization is (are) _____

I understand that I have the right to inspect and copy the information I have authorized to be disclosed by this authorization. In the event I refuse to authorize the release of the above-described information, I understand that it will not be disclosed, except as provided by law.

I understand that the practice may not condition treatment on whether I sign this authorization, except when the provision of health care is solely for the purpose of creating protected health information for disclosure to a third party.

I understand that information used or disclosed pursuant to this authorization may be subject to redisclosure by the recipient and may no longer be protected by law.

I understand that this authorization is valid until it expires, unless revoked before that.

I understand that I may revoke this authorization at any time by giving written notice to the physician of my desire to do so. I also understand that I will not be able to revoke this authorization in cases where the physician has already relied on it to use or disclose my health information. Written revocation must be sent to the physician's office. Absent such written revocation, this Authorization for Release of Confidential Health Information will terminate on _____.

(Date)

Signed: _____ Date: _____

If you are not the patient, please specify your relationship to the patient: _____.

Individual Rights – Waiver of Rights

Background

One section of the Privacy Rule addresses the waiver of individual rights.⁸ In general, a covered entity – including a physician – may not require individuals to waive any of their individual rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

Model Policy

The practice never requires an individual to waive any of his or her individual rights as a condition for the provision of treatment, except under very limited circumstances allowed under law and referenced elsewhere in these policies and procedures.

Model Procedure

The practice allows every individual to enforce all of the rights described in the practice's policies and procedures manual and does not, in any way require or encourage an individual to waive any of those rights as a condition for the provision of treatment, except as allowed by law and noted elsewhere in these policies and procedures.

⁸ § 164.530(b) – Administrative Requirements – Standard – Waiver of Rights.

Uses and Disclosures of Protected Health Information

Uses and Disclosures – Verification of Identity

Background

Five sections of the regulations address the release of PHI to appropriate individuals.⁹ A covered entity – including a physician – must reasonably ensure that PHI is only used by and released to appropriate individuals. This requires verification of the identity of the individual using or receiving the information.

Model Policy

The practice makes reasonable efforts to ensure that protected health information (PHI) is only used by and disclosed to individuals that have a right to the PHI. Toward that end, the practice makes reasonable efforts to verify the identity of those using or receiving PHI.

Model Procedure

The practice normally verifies the identity of individuals based on a known:

- place of business;
- address;
- telephone (including the use of caller ID) or fax number; or
- person.

Verification of Public Officials: The practice relies on information provided by a public official, if such reliance is reasonable, and:

- if the request is made in person, accompanied by an agency identification badge, other official credentials, or other proof of government status;
- if the request is in writing, the request is on the appropriate government letterhead; or
- if the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's

⁹ § 164.514(h) – Other Procedural Requirements Relating to Uses and Disclosures of Protected Health Information – Standard – Verification Requirements; § 164.512(a) – Uses and Disclosures for which Consent, an Authorization or Opportunity to Objection is Not Required – Standard – Uses and Disclosures Required by Law; § 164.512(f) – Uses and Disclosures for which Consent, an Authorization, or Opportunity to Agree or Object is Not Required – Standard – Disclosures for Law Enforcement Purposes; § 164.502(f) – Uses and Disclosures of Protected Health Information – General Rules – Standard – Deceased Individuals; and § 164.510(b) – Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object – Standard – Uses and Disclosures for Involvement in the Individual's Care and Notification Purposes.

authority, or other evidence or documentation of such authority such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

The practice relies, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of PHI is to a public official or a person acting on behalf of the public official:

- a written statement of the legal authority under which the PHI is requested or
- if a request is made pursuant to legal process, a warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal it is presumed to constitute legal authority.

Further information about when a disclosure is required by law is discussed under Uses and Disclosures – Required by Law (see Uses and Disclosures Required by Law, page 51).

Disclosure to the Secretary of the U.S. Department of Health and Human Services is required for purposes of enforcing the Privacy Rules. When the Secretary for compliance purposes requests PHI, the practice verifies the same information that is required for other law enforcement or oversight requests for disclosure.

Emergency Situations: If there is an imminent threat to safety, the practice will disclose PHI to prevent or lessen a serious and imminent threat to the health or safety of a patient if disclosure is made to a person reasonably able to prevent or lessen the threat. In such emergencies, the practice does not demand written proof that the person requesting the PHI is legally authorized. The practice reasonably relies on the verbal representations of the parties involved.

Verification of Persons Assisting in an Individual's Care: In most instances, it is expected the practice will know the identity of persons assisting in an individual's care, e.g., a parent, a child, or a spouse. In all other instances, the practice takes reasonable steps to verify the identity of the individual assisting in the care, including provision of government-issued photo identification.

Verification of an Individual Requesting Their PHI: The practice gives an individual access to his or her PHI in most instances (see Individual Rights – Inspect and Copy PHI, page 17). In most instances it is expected the practice knows each individual requesting his or her PHI. In all other instances, the practice takes reasonable steps to verify the identity of the individual making the request, including provision of government-issued photo identification.

Verification of a Personal Representative: The practice may release PHI to a personal representative. If a person's status as personal representative hasn't already been established, the practice:

- requires a power of attorney for healthcare;
- a copy of a guardianship order; or
- asks questions to determine that an adult acting for a young child has the requisite relationship to the child, e.g., parent, guardian, or an adult with written authorization from the parent or guardian.

Verification for Use for Research Purposes: The practice does not release PHI for research purposes. (See Research Activities, page 59.)

Verification of Family Member: Only when authorized by law, the practice discloses PHI to family members when, in the exercise of professional judgment, the practice believes the disclosure is in the individual's best interest and when the individual is not available to agree to the disclosure or is incapacitated. When the practice is not already aware of the relationship to the individual, the practice seeks positive verification of the relationship to the individual.

Disclosed to Other Entities: The practice makes a reasonable effort to determine that PHI sent to other entities is only disclosed to individuals authorized to receive it. Sending the information to a recognizable organizational address, or if faxing or phoning information, by calling the requester back through the main organization switchboard rather than through a direct phone number, is deemed sufficient to meet the requirement of the Privacy Rule. (See Physical Safeguards – Records Processing – Receiving, Sending, and Disposing of PHI, page 81.)

Uses and Disclosures – Personal Representatives

Background

Four sections of the regulations address the release of PHI to personal representatives.¹⁰ In general, a covered entity – including a physician – must, with two exceptions, treat a personal representative as the individual. The rule gives specific guidelines for personal representatives, adults and emancipated minors, unemancipated minors, deceased individuals, and abuse, neglect, and endangerment situations.

Model Policy

For disclosure and other purposes, the practice treats all individuals properly qualified or designated as personal representatives of patients the same as if that individual were the patient.

Model Procedure

The practice generally allows properly qualified or designated individuals to act as personal representatives of patients. The two general exceptions to allowing individuals to act as personal representatives relate to unemancipated minors and abuse, neglect, or endangerment situations.

Individuals who may serve as personal representatives are limited to the following:

- an attorney-in-fact under a Power of Attorney for Health Care;
- a court-appointed guardian with authority to access medical records or make health care decisions;
- a parent or other authorized adult acting on behalf of the parent; and
- an individual with written authorization, from a competent adult patient, to access medical records.

See also the section on Deceased Individual's PHI, page 57.

Abuse, Neglect, and Endangerment Situations: The practice does not treat an individual as a personal representative of a patient if:

- in the professional judgment of the practice, the patient has been or may be subjected to domestic violence, abuse, or neglect by the individual; or
- in the professional judgment of the practice, treating the individual as the personal representative could endanger the patient and the practice decides it is not in the best interest of the patient to treat the individual as the patient's personal representative.

¹⁰ § 164.502(g) – Uses and Disclosures of Protected Health Information – General Rules – Standard – Personal Representatives; § 164.524 – Access of Individuals to Protected Health Information; § 164.528 – Accounting of Disclosures of Protected Health Information; and § 164.510(b) – Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object – Standard – Uses and Disclosures for Involvement in the Individual's Care and Notification Purposes.

Unemancipated Minors: The practice treats as a personal representative a parent, guardian, or other person acting *in loco parentis* if, under applicable law, the parent, guardian, or other person acting *in loco parentis* has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care. However, the practice does not treat such a person as personal representative of an unemancipated minor, and the minor has the authority to act as an individual, if:

- the minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting *in loco parentis*, and the minor, a court, or another person authorized by law consents to such health care service; or
- a parent, guardian, or other person acting *in loco parentis* assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

The practice will not disclose PHI to a parent, guardian, or other person acting *in loco parentis* if:

- such disclosure is prohibited by state or other law, including applicable case law; or
- such action is inconsistent with state or other applicable law, in the professional judgment of the practice.

South Dakota law prohibits disclosure of the minor's PHI without consent if the minor is emancipated, whether by marriage, court order, or otherwise. Except in certain circumstances, South Dakota law requires 48 hours' prior written notice to the parent or guardian of an unemancipated minor or to the guardian of an incompetent adult of the person's request for an abortion. A parent or guardian need not be notified if the treating physician believes that a medical emergency exists or if the patient asks that a parent or guardian not be informed, in which case a court order is necessary. In these circumstances, the Privacy Rule defers to State law as to the issues of notice to a parent or guardian and the minor patient's right to demand that a parent or guardian not be notified.

Adults: The practice treats a person as a personal representative of an adult if, under applicable law, the person has authority to act on behalf of the adult in making decisions related to health care.

Deceased Individuals: The practice treats an executor, administrator, or other person in the same manner that they would have treated a patient, were the patient not deceased, if under applicable law, the executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate.

Uses and Disclosures – Not Requiring Authorization

Disclosure to Those Involved in Individual's Care

One section of the regulations addresses the disclosure of PHI to those involved in an individual's care.¹¹ Generally, a covered entity – including a physician – is required to disclose PHI to family members, close friends, or other persons assisting in an individual's care, as well as government agencies and disaster relief organizations conducting disaster relief activities. The disclosure may result from an oral agreement, without written authorization, so long as the covered entity informs individuals in advance of such use or release and provides a meaningful opportunity for the individual to prevent or restrict the disclosure. (This restriction does not apply in emergency situations. See Uses and Disclosures in Emergency Situations, page 55.)

Model Policy

The practice discloses PHI to those involved in a patient's care when the patient approves or, when the patient is not present or not able to approve, when such disclosure is deemed appropriate in the professional judgment of the practice.

Model Procedures

Disclosure When Patient is Present: When the patient is present and has the capacity to make his or her own decisions, the practice discloses PHI only if:

- the patient agrees to the disclosure to the third parties involved in their care, and the patient is provided with an opportunity to object to such disclosure and does not express an objection; or
- it is reasonably inferred from the circumstances, based on professional judgment, that the patient does not object to the disclosure, such as when a patient brings a spouse into the doctor's office when treatment is discussed or when a parent, child, colleague or friend has brought the subject to the emergency department for treatment.

Generally the practice will:

- not verify the identity of relatives or others involved in a patient's care. The patient's act of involving the other persons in his or her care suffices as verification of their identity; and
- use and release information on an episodic basis. It is not assumed that agreement at one point in time to disclose PHI to a relative or to another person implies agreement to disclose PHI in the future.

Disclosure When Patient is Not Present: When the patient is not present, the practice determines whether the disclosure of the patient's PHI is authorized by law, and if so, discloses

¹¹ § 164.510(b) – Uses and Disclosures for Involvement in the Individual's Care and Notification Purposes – Standard.

only the PHI directly relevant to the person's involvement with the patient's health care. Among other things, the practice:

- discloses functional information to individuals assisting in a patient's care (for example, disclosing mobility limitations to a friend driving the patient home from the practice); and
- allows an individual to act on the patient's behalf to pick up medical supplies, X-rays, and similar forms of PHI with permission of the patient.

The practice does not disclose PHI to a suspected abuser, if, in its professional judgment, there is reason to believe that such a disclosure could cause the patient serious harm. Further, the practice uses and discloses information as required by law (see Uses and Disclosures Required by Law, page 51).

Uses and Disclosures Required by Law

Five sections of the regulations address the provision of PHI as required by law.¹² Generally, a covered entity – including a physician – is required to use and disclose PHI as required by federal, state, and local laws.

NOTE: Several portions of the regulations deal with the preemption of state law.¹³ The following model procedure relies on a preemption analysis completed by counsel for the South Dakota State Medical Association. This means that the federal HIPAA requirements sometimes are changed by South Dakota law. In such instances, these Model Policies and Procedures reflect South Dakota law, taking into account of the federal HIPAA requirements.

Model Policy

The practice uses and discloses protected health information (PHI) to appropriate individuals as required by law.

Model Procedure

The practice:

- ensures that the use or disclosure is, in fact, required by law;
- ensures that the use or disclosure meets the requirements of the law and is limited to what is relevant to the law;
- specifically addresses the types of disclosures required by law for which additional requirements apply (discussed below);

¹² § 164.501 – Definitions – Required by Law; § 164.512 – Uses and Disclosures for which Consent, an Authorization, or Opportunity to Agree or Object is Not Required; § 164.502(b)(2)(iv) – Standard – Minimum Necessary Does Not Apply; § 164.514(d)(3)(iii)(A) – Implementation Specification – Minimum Necessary Disclosures of Protected Health Information; and § 164.514(h)(1) – Verification Requirements.

¹³ § 160.201 – Applicability; § 160.202 – Definitions; § 160.203 – General Rule and Exceptions; § 160.204 – Process for Requesting Exception Determinations; and § 160.205 – Duration of Effectiveness of Exception Determinations.

- provides a process for applying professional judgment regarding waiving individual notification, such as for victims of abuse, neglect, or domestic violence (discussed below);
- relies on the public official making a request that the request is for the minimum amount of PHI necessary for the official's lawful purpose; and
- verifies the identity of an individual requesting PHI and his or her authority to have access to such information (see Uses and Disclosures – Verification of Identity, page 45).

Uses and Disclosures Required by Law: The practice uses and discloses PHI as required by law and detailed below. The specific reasons for releasing PHI as required by law are discussed below. These disclosures are not subject to the minimum necessary requirements (see Uses and Disclosures – Minimum Necessary, page 61), but will be limited to disclosures that comply with and are relevant to the requirements of law.

Disclosures for Public Health Activities: As required by law, the practice discloses PHI to public health officials. This includes reporting of:

- identifiable and suspected cases of communicable diseases;
- cases of venereal disease;
- cases of ophthalmia neonatorum;
- cases of known or suspected severe auditory or visual impairment suffered by a minor child.

Disclosures about Victims of Abuse, Neglect, or Domestic Violence: The practice discloses PHI regarding minors who are victims of abuse, neglect, or domestic violence.

The practice informs the individual of the reporting unless the practice, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm, or if the practice would be informing a personal representative and the practice believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by the professional judgment of the practice.

Uses and Disclosures for Health Oversight Activities: The practice uses and discloses PHI as required by law for health oversight activities. The information may be used and released for audits, investigations, licensure issues, and other health oversight activities, including, but limited to:

- hospital peer review;
- managed care peer review; or
- Medicaid or Medicare peer review.

Disclosures for Judicial and Administrative Proceedings: The practice discloses information for judicial and administrative proceedings in response to:

- an order of a court or administrative tribunal (disclosure is limited to PHI expressly authorized by the order); or
- a subpoena, discovery request, or other lawful process not accompanied by an order of a court or administrative tribunal, if :
 - the practice is satisfactorily assured that the individual has been given notice of the request (the party seeking the PHI provides a written statement to the practice with documentation demonstrating the individual has been contacted or attempted to be contacted, that the notice to the individual was descriptive enough to permit the individual to raise an objection to the proceeding, and the time for objections has elapsed and no objections were filed or filed objections were resolved and disclosures are consistent with resolution), or
 - the practice is satisfactorily assured that the party seeking information has made reasonable efforts to receive a qualified protective order (the party seeking the PHI provides a written statement to the practice with documentation demonstrating that the parties to the dispute have agreed to and presented a qualified protective order to the court or administrative tribunal or the party seeking the PHI has requested a qualified protective order from such court or administrative tribunal).

NOTE: The practice should obtain these written assurances, or the individual's written authorization, prior to complying with a subpoena, discovery request, or other lawful process.

Disclosures for Law Enforcement Purposes: The practice discloses PHI for law enforcement purposes to law enforcement officials.

- The practice releases PHI pursuant to a process and as otherwise required by law if the information sought is relevant and material, the request is specific and limited to amount reasonably necessary, and it is not possible to use de-identified information.
- The practice releases limited PHI as provided in the Privacy Rule to identify or locate a suspect, fugitive, material witness, or missing person only as approved by a person authorized to act on behalf of the individual.
- The practice discloses limited PHI as provided in the Privacy Rule about a suspected victim of a crime if the individual who is the subject of the crime agrees to disclosure.
- The practice discloses PHI about a deceased individual if the practice suspects that death resulted from criminal conduct and such disclosure is approved by persons authorized to act on behalf of the deceased individual.
- The practice discloses PHI that the practice judges to constitute evidence of criminal conduct that occurred on the covered entity's premises.
- The practice discloses PHI relating to the provision of emergency health care as required or permitted by law such as test results of those involved in automobile or boating accidents.
- The practice may disclose PHI when the practice has reasonable cause to believe the patient's ability to safely drive may be impaired to the point where it constitutes a serious and imminent threat to the health or safety of a person or the public.

Uses and Disclosures Related to Decedents: The practice uses and discloses PHI as required to a coroner or medical examiner and funeral directors as required by law. The attending physician is required to sign the death certificate and provide the coroner with a copy of the decedent's PHI.

Uses and Disclosures Related to Cadaveric Organ, Eye or Tissue Donations: The practice uses and discloses PHI to facilitate organ, eye, or tissue donations.

Uses and Disclosures for Research Purposes: The practice does not participate in any research studies. Accordingly, the practice does not use or disclose any PHI for research purposes. (See Research Activities, page 59.)

Uses and Disclosures to Avert a Serious Threat to Health or Safety: The practice uses and discloses PHI to public health and other authorities as required by law to avert a serious threat to health or safety.

Uses and Disclosures for Specialized Government Functions: The practice uses and discloses PHI for military and veterans' activities, national security and intelligence activities, and other activities as required by law.

Documentation

The practice documents disclosures required by law on the Disclosures of PHI Tracking Log, page 15. This information is retained as required under section § 164.630(j) for a period of six years from the date of its creation.

NOTE: This requirement may in some circumstances change the record retention periods for medical records under South Dakota law. See SDCL 36-4-37 and 36-4-38.

Uses and Disclosures in Emergency Situations

Six sections of the regulations address the provision of PHI in emergency situations.¹⁴ Generally, a covered entity – including a physician – is allowed to use and disclose PHI in emergency situations without providing the covered entity’s Notice of Privacy Practices to the individual. As soon as possible after the use or disclosure of PHI in emergency situations, the covered entity should provide the Notice to direct treatment patients.

Model Policy

The practice uses and discloses protected health information (PHI) as appropriate to provide treatment in emergency situations. In those instances where the practice has not previously provided its Notice of Privacy Practices to a patient who receives direct treatment in an emergency situation, the practice provides the Notice to the individual as soon as practicable following the provision of the emergency treatment.

Model Procedures

The practice:

- uses and discloses PHI as appropriate to provide treatment in an emergency situation; and
- in the case of a direct treatment patient who has not previously received its Notice of Privacy Practices, the practice provides the Notice to the individual as soon as practicable following the provision of the emergency treatment.

Marketing Purposes

Three sections of the regulations address the use and disclosure of PHI for marketing purposes.¹⁵ Generally, a covered entity – including a physician – must limit the use and disclosure of PHI for marketing purposes, unless the patient signs an authorization allowing such use and disclosure.

Model Policy

The practice does not use or disclose any protected health information (PHI) for marketing purposes.

¹⁴ § 164.506(a) Standard – Consent Requirement; § 164.506 (a)(3)(i)(A) – Consent During Emergency Treatment Situations §164.510(b)(3) – Limited Uses and Disclosures When the Individual is Not Present; § 164.512(f)(3) – Permitted Disclosure – Victims of a Crime; § 164.512(f)(6) – Permitted Disclosure – Reporting Crime in Emergencies; § 164.512(j) – Permitted Disclosure – To Avert a Serious Threat to Health or Safety; and § 164.522(a)(1) – Standard – Right of an Individual to Request Restriction of Uses and Disclosures.

¹⁵ § 164.501 – Definitions – Marketing; § 164.508(a) – Uses and Disclosures for Which Authorization is Required – Standard – General Rules; and § 164.508(b) – Implementation Specifications for Authorizations.

NOTE: If the practice is planning to use or disclose PHI for marketing purposes, this policy and the accompanying procedures will have to be modified significantly.

Model Procedures

Marketing is defined in the Privacy Rule as follows:

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

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

(ii) For treatment of the individual; or

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

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

The practice *does* engage in communications about products and services that encourage recipients of the communication to purchase or use the product or service for treatment or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual. As defined above, these activities are not marketing.

De-Identification of PHI

Four sections of the regulations deal with the provision of “de-identified” PHI.¹⁶ Generally, a covered entity – including a physician – may disclose “de-identified” PHI, so long as the covered entity meets the requirements for de-identifying PHI as outlined in the Privacy Rule which requires in part that PHI be stripped of 18 data elements. The process of de-identifying

¹⁶ § 164.502(d) – Uses and Disclosures of Protected Health Information – Standard – Uses and Disclosures of De-identified Protected Health Information; § 164.514(a) – Other Requirements Relating to Uses and Disclosures of Protected Health Information – Standard – De-identification of Protected Health Information; § 164.514(b) – Other Requirements Relating to Uses and Disclosures of Protected Health Information – Implementation Specifications – Requirements for De-identification of Protected Health Information.; and § 164.514(c) – Re-identification of Information.

information is very complex, and most physician practices have no need to release de-identified information.

Model Policy

The practice does not de-identify PHI and, as such, does not release any de-identified protected health information (PHI).

Deceased Individual's PHI

Three sections of the regulations address the provision of PHI of deceased individuals.¹⁷ In general, a covered entity – including a physician – must protect the PHI of a deceased individual for as long as the covered entity maintains the PHI. The covered entity may disclose a decedent's PHI to coroners, medical examiners, and funeral directors as required by law (see Deceased Individual's PHI, page 57). In addition, the covered entity must treat individuals lawfully representing decedents as if the deceased individuals were still alive.

Model Policy

The practice protects PHI regarding a deceased individual and only discloses PHI regarding a deceased individual as required or permitted by law.

Model Procedure

The practice:

- protects the PHI of a deceased individual in the same manner and to the same extent as required for the PHI of living individuals, except for uses and disclosures for research purposes;
- may use and disclose the PHI of deceased persons for research purposes without obtaining authorization from a personal representative and absent approval by an IRB or privacy board if the researcher represents that the use or disclosure is sought solely for research on the PHI of decedents and documentation is provided, at the request of the practice, of the death of such individuals and representation is provided that the PHI which is sought is necessary for the research purposes;
- treats an executor, administrator, or other person who has authority to act on behalf of a deceased individual as a personal representative with respect to PHI and as such treats the personal representative of an individual in the same manner they would have treated the deceased individual when they were alive;
- discloses PHI about a deceased individual to coroners and medical examiners for identification of a deceased person or to determine cause of death (This disclosure may occur prior to and in reasonable anticipation of the individual's death.); and

¹⁷ § 164.502(f) – Uses and Disclosures of Protected Health Information – General Rules – Standard – Deceased Individuals; § 164.502(g)(4) – Uses and Disclosures of Protected Health Information – General Rules – Standard – Personal Representatives – Implementation Specification – Deceased Individuals; and § 164.512(g) – Uses and Disclosures for which Consent, an Authorization, or Opportunity to Agree or Object is Not Required – Standard – Uses and Disclosures About Decedents.

- discloses PHI about a deceased individual to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to a decedent (These disclosures may occur prior to and in reasonable anticipation of the individual's death.).

Uses and Disclosures – Do Not Apply to Practice

Research Activities

PHI created for research is subject to the Privacy Rule requirements.¹⁸ This is a particularly complex area of the regulations. To simplify these model policies and procedures, it is recommended that physicians at this time not participate in any research studies that involve PHI.

Model Policy

The practice does not engage in any research activities that require it to use or disclose protected health information.

NOTE: If a practice does engage in research activities, they are encouraged to seek guidance with respect to the HIPAA Privacy Rules from those leading the research. They should be able to provide you with the necessary protocols, including all forms and assurances, required for you to use and disclose PHI for research purposes.

Keep in mind that the research entity may *not* be covered under HIPAA and may not have to meet the HIPAA privacy requirements. In any case, you need to make sure work with the research entity to ensure all research in which you are involved meets all HIPAA requirements.

You will need to make sure that you modify your policies and procedures to describe the specific research project and to incorporate the research protocol as it applies to your practice and your patients. This may include: reference to a research-specific authorization form, a description of the confidential information being collected for the research, when and under what circumstances confidential information will be released in connection with the research, the length of the research project, and whether patients are entitled to their confidential information related to the research during the course of the research.

You will need separate policies and procedures for each research project in which you participate.

¹⁸ § 164.506 – Consent for Uses or Disclosures to Carry Out Treatment, Payment, or Health Care Operations; § 164.508 – Uses and Disclosures for which an Authorization is Required; § 164.512(i) – Uses and Disclosures for which Consent, an Authorization, or Opportunity to Agree or Object is Not Required Including the Standards for Uses and Disclosures for Research Purposes; § 164.524 – Access of Individuals to Protected Health Information; and § 164.532 – Transition Provisions.

Other Uses and Disclosures

Several other uses and disclosures in the Privacy Rule generally do not occur in small provider practices. These include:

- disclosure to an employer or health plan sponsor¹⁹;
- use and disclosure for underwriting and related purposes²⁰;
- use and disclosure for facility directories²¹;
- use and disclosure to brokers and agents²²; and
- use for fundraising.²³

Model Policy

The practice does not use or disclose protected health information (PHI) to an employer or health plan sponsor for underwriting and related purposes, for facility directories, to brokers and agents, or for fundraising.

Model Procedures

If an individual wants the practice to release his or her PHI to employers or health plan sponsors, for underwriting and related purposes, for facility directories, or to brokers and agents, he or she can contact the practice and complete an appropriate written authorization (see Individual Rights – Authorizations, page 38).

¹⁹ § 164.504 – Uses and Disclosures: Organizational Requirements.

²⁰ § 164.508(a) – Uses and Disclosures for which Authorization is Required – Standard – General Rules; § 164.508(b)(4)(A) and (B) – Prohibition on Conditioning of Authorizations (*exceptions*); § 164.514(g) – Other Requirements Relating to Uses and Disclosures of Protected Health Information – Standard – Uses and Disclosures for Underwriting and Related Purposes; § 164.504(f) – Uses and Disclosures: Organizational Requirements (*standard requirements for group health plans*); and § 164.528 – Accounting of Disclosures of Protected Health Information.

²¹ § 164.510(a) – Use and Disclosure for Facility Directories – Standard.

²² § 164.504(f) – Requirements for Group Health Plans; § 164.510(b)(2) – Uses and Disclosures with the -Individual Present; and § 164.510 – Uses and Disclosures for which an Authorization is Required.

²³ § 164.508(a) – Uses and Disclosures for which Authorization is Required – Standard – General Rules; § 164.508(b) – Implementation Specifications for Authorizations; § 164.514(e) – Standard – Uses and Disclosures of Protected Health Information for Marketing; and § 164.514(f) – Standard: Uses and Disclosures of Protected Health Information for Fundraising.

Uses and Disclosures – Minimum Necessary

Background

Two sections of the regulations address the minimum necessary requirements.²⁴ As stated in the Privacy Rule:

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

Minimum necessary does **NOT** apply in the following situations:

- disclosures or requests by a health care provider for treatment;
- uses or disclosures made to the individual permitted under the regulations or authorized by the individual;
- disclosures made to the Secretary;
- uses or disclosures required by law; and
- uses or disclosures required to comply with the Privacy Rule.

Model Policy

The practice reasonably ensures that the protected health information (PHI) it requests, uses, and discloses for any purpose is the minimum amount of PHI necessary for that purpose.

Model Procedure

Exceptions: The practice recognizes that the minimum necessary restrictions do not apply to:

- disclosures or requests by a health care provider for treatment;
- uses or disclosures made to the individual permitted under this section or authorized by the individual;
- disclosures made to the Secretary;
- uses or disclosures required by law (although the disclosure must still be limited to what is required by, and is relevant to, the law in question); and
- uses or disclosures required to comply with the Privacy Rule.

Uses of PHI: The practice has a very small workforce. Everyone in the office is responsible for every task from time to time. Accordingly, everyone in the office has a need to review all PHI. The practice allows all members of its workforce to have access to all PHI as is necessary for

²⁴ § 164.502(b) – Uses and Disclosures of Protected Health Information: General Rules – Standard – Minimum Necessary; and § 164.514(d) – Other Requirements Relating to Uses and Disclosures of Protected Health Information – Standard – Minimum Necessary Requirements.

them to carry out their job functions. The practice limits access to PHI to that information necessary for a member of its workforce to carry out his or her job functions. The amount and type of PHI necessary to carry out job functions varies depending on the specific tasks assigned to the member of the workforce each day depending on the needs of the practice.

Disclosures of PHI: The practice limits the PHI it discloses to that necessary to meet the purpose of the disclosure. For disclosures for:

- payment, the practice releases the information required to file a claim and, if requested, additional information requested by a third party payer to adjudicate the claim (psychotherapy notes are not released without authorization for payment purposes); and
- health care operations, the practice releases the specific information required by the entity engaging in the health care operations, e.g., utilization review, quality assurance.

NOTE: The practice should list additional routine disclosures that it makes. For example, if the practice discloses information to a transcription service, accountant, or practice management company, it should specify the kinds of information disclosed.

The practice reviews such routine requests to ensure that they are reasonable and do not seek PHI beyond that reasonably required by the requestor to complete the purpose of the request. If, in the opinion of the practice, the requestor has requested more information than necessary, the practice so notifies the requestor and seeks clarification regarding what PHI the requestor actually needs.

The practice relies on a request for disclosure as being for the minimum necessary amount of information if:

- the disclosure is to a public official and the public official represents that the request is for the minimum necessary information;
- the request is from another covered entity – a health care provider, health plan, or clearinghouse; or
- the request is from a business associate in order to provide a professional service to the practice and the professional represents that the request is for the minimum necessary information.

For non-routine disclosures, the Privacy Officer reviews the request and determines if, in the professional judgment of the practice, the disclosure is for the minimum amount of information necessary to carry out its purpose.

Requests for PHI: The practice sometimes has a need to request PHI from other entities, particularly other health care providers. In such instances, the practice limits its request to that information that is “reasonably necessary” to accomplish the purpose of the request. For routine, recurring requests, the practice describes the information being requested and purpose for the request.

Most often the practice requests information related to the treatment of a patient. The minimum necessary requirements do not apply when the request is for purposes of treatment of a patient.

Use and Disclosure of Medical Record: The practice limits the use, disclosure, or request for a medical record to what is specifically needed in the professional judgment of the practice. For example, if there is a question regarding payment for a practice service, only the portion of the medical record related to that service is released.

The practice does not routinely use or disclose the entire medical record unless such use or disclosure is necessary. If requested by a health care provider, the entire medical record is made available to those involved in the treatment of the patient. Further, a patient (or his or her personal representative) may request his or her designated record set (the patient's medical record and billing record).

Uses and Disclosures – Business Associates

Three sections of the Privacy Rule and three sections of the Security Rule address the release of PHI to business associates.²⁵ In general, a covered entity – including a physician – must enter into a Business Associate Agreement with any person who acts in a capacity other than as a member of the workforce of a covered entity to perform or assist in the performance of a function or activity on behalf of the covered entity involving the use or disclosure of PHI or any other function or activity otherwise governed by the Privacy Rule.

Model Policy

The practice identifies business associates and enters into Business Associate Agreements with all of its business associates.

Model Procedure

When the practice discloses protected health information (PHI) to any entity for any purpose, the practice considers whether the PHI is being released to:

- the patient or a personal representative of the patient;
- to a person as authorized by the patient or the patient’s personal representative;
- to another covered entity;
- to a person as required by law; or
- to some other person acting on behalf of the practice. Such other persons shall be considered business associates.

Business associates may include practice management companies, billing services, legal and accounting services, computer vendors which utilize your PHI, financial services, and medical liability insurance companies.

The practice requires each of its business associates to sign a Business Associate Agreement with the practice. The Business Associate Agreement complies with the requirements of the Privacy Rule and Security Rule and ensures that PHI shared with the business associate remains private and secure.

NOTE: A Model Business Associate Agreement is attached to this document (see page 140).

²⁵ § 160.103 – Definitions – Business Associates; § 164.308(b)(1) – Standard – Business Associate Contracts; § 164.314(a) – Standard and Implementation Specification – Business Associate Contracts and Other Arrangements; § 164.316 – Policies and Procedures and Documentation Requirements; § 164.502(e) – Uses and Disclosures of Protected Health Information – General Rules – Standard – Disclosures to Business Associates; and § 164.504(e) – Uses and Disclosures – Organizational Requirements – Standard: Business Associate Contracts.

Security Policies and Procedures

The Security Proposed Rule was issued in 1999. The Security Final Rule was issued February 20, 2003, and its compliance date is April 2005. It applies to the security of electronic information.

The Final Privacy Rule includes section 164.530(c)(1) – Administrative requirements; Standard: Safeguards. This provision states that “[a] covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.” In addition, it adds “[a] covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications, or other requirements of this subpart.”

In other words, even though the Security Final Rule does not have to be complied with until April 2005, a practice must implement security policies and procedures now to safeguard its protected health information – both paper and electronic – to comply with the Privacy Rule.

This section presents model security policies and procedures. ISMS and ISMIE Mutual developed these model policies and procedures to enable their members and policyholders, particularly small practices, to come into compliance with the HIPAA Privacy Rule. It is used with permission of ISMS and ISMIE and has been modified for South Dakota practitioners.

These model policies and procedures reflect the requirements in the Security Rule. The requirements are placed in three categories:

- administrative safeguards addressing the administrative policies and procedures that need to be developed and implemented;
- physical safeguards addressing the physical aspects of security that need to be addressed; and
- technical safeguards addressing the computer programs and other processes that need to be implemented.

In each of these areas there are a number of requirements. In addition, some of the requirements overlap, e.g., the assignment and use of passwords is an administrative safeguard that is implemented using a software program (technical safeguard). Where possible, requirements that overlap are consolidated.

NOTE: The model policies and procedures must be reviewed by each practice and modified as necessary. You must determine if and how these model policies and procedures apply to your practice, modify them so they do reflect your practice, and make any necessary changes to ensure your practice is in compliance with the HIPAA Security Rules.

You must meet the requirements of the Security Final Rule by April 2005. The model policies and procedures in this document are consistent with the final rule

and implement the requirements of the final rule.

NOTE: These model policies and procedures are copyright by ISMS/ISMIE Mutual Insurance Co. Permission is granted to ISMS members and ISMIE Mutual Co. policyholders to use and modify these model policies and procedures so that they can bring their practices into compliance with HIPAA.

Permission also is granted to members of the South Dakota State Medical Association to use and modify these model policies and procedures so that they can bring their practices into compliance with HIPAA.

Other individuals and groups wishing to use or modify these model policies and procedures must seek written permission from ISMS/ISMIE Mutual Insurance Co. and pay a royalty to ISMS/ISMIE Mutual Insurance Co.

NOTE: This document does not constitute legal advice. You are urged to seek legal advice if you have any questions regarding how HIPAA applies to your practice.

Administrative Safeguards

Numerous sections of the final Security Rule address administrative safeguards. The rule defines administrative safeguards as “actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity’s workforce in relation to the protection of that information.”

Small practices are required to implement appropriate policies and procedures to protect their protected health information (PHI) – confidential information – and ensure that it remains secure. Recall that the Security Rule only covers electronic information. The Privacy Rule also addresses confidential information kept in paper and other forms. In order to meet the Privacy Rule requirements, the practice also must protect paper-based information.

The following portions of this document address the administrative safeguard policies and procedures that practices need to consider when implementing HIPAA privacy and security. Several of the Security Rule administrative requirements are included in these Model Policies and Procedures under the heading of “Administrative Policies and Procedures” (see page 98).

Administrative Safeguards – Risk Analysis, Risk Management, and Ongoing Risk Evaluation

Background

Three sections of the Security Rule address risk analysis, risk management, and evaluation.²⁶ In general, a covered entity – including a physician – must conduct a risk analysis and ongoing evaluations to identify potential security risks and to determine how to address significant risks.

Model Policy

The practice has undertaken an initial risk analysis and ongoing evaluations to identify potential risks and to identify how to manage significant risks.

Model Procedures

NOTE: This section is written on the assumption that you have completed the Small Practice Security Risk Analysis, page 128.

Risk Assessment: The practice has completed an initial risk analysis (Small Practice Security Risk Analysis, page 128). As required by the final rule, this risk analysis provided an “accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the” practice. Recognizing that the Privacy Rule requires the practice to protect paper and oral PHI as well as electronic, this risk assessment addressed the full range of PHI held by the practice.

Evaluation: The practice undertakes an evaluation of its security annually. This evaluation involves updating the risk analysis to ensure that all potential risks are identified and identifying any new or evolving risks that need to be managed.

In addition to the periodic scheduled evaluations, the practice completes an evaluation wherever there is a significant change to any of its systems, e.g., new programs or hardware are implemented, physical plant, e.g., space is added or modified, or administrative operations, e.g., the flow of information in the office is modified.

Risk Management: On the basis of the risk assessment and the ongoing evaluations, the practice adequately manages its risks. The policies and procedures included in this manual reflect the actions taken by the practice to manage its risk.

²⁶ § 164.308(a)(8) – Standard – Evaluation; § 164.316(a)(2)(i) – Implementation Specification – Risk Analysis; and § 164.316(a)(2)(ii) – Implementation Specification – Risk Management.

Administrative Safeguards – Contingency Planning

Background

Eight sections of the Security Rule address contingency planning.²⁷ In general, a covered entity – including a physician – must have in place contingency plans to ensure mission critical electronic-based information is available in a timely fashion.

Model Policy

The practice has in place appropriate contingency plans so that it can continue to provide critical functions if it is faced with a loss of access to electronic-based protected health information (PHI).

Model Procedures

Criticality Analysis: The practice keeps logs of its devices and media (Device and Media Controls Log, page 90) and the software on each of its devices that may contain PHI (see “PHI” Software Log, page 72). These logs note which systems contain PHI and specifically which files contain PHI so that those files can be backed up and are maintained by the Security Officer.

The practice does not store its medical records electronically [*or keeps paper copies of all medical records*]. Accordingly, the recovery of lost electronic-based PHI is not time-critical to patient care.

<p>NOTE: If a practice has electronic medical records and does not keep paper copies of those medical records, this section will need to be expanded. The criticality analysis will have to document which systems are necessary to ensure timely patient care.</p>
--

Data Backup Plan: The practice backs up all PHI maintained on its computer systems. The information is backed up on a weekly basis to a [*insert media type, e.g., diskettes, Zip Drive, CD*]. The information is password protected. Two copies are made. One copy is stored at the practice and the second copy is stored offsite. In an emergency, the information is backed up as soon as possible and removed offsite. In addition, PHI is backed up prior to moving any computer or modifying any software containing PHI. Backups are recorded on the Backup Log, page 73.

²⁷ § 164.308(a)(7)(i) – Administrative Safeguards – Standard: Contingency Plan; § 164.308(a)(7)(ii)(A) – Administrative Safeguards – Implementation Specifications – Data Backup Plan; § 164.308(a)(7)(ii)(B) – Administrative Safeguards – Implementation Specifications – Disaster Recovery Plan; § 164.308(a)(7)(ii)(C) – Administrative Safeguards – Implementation Specifications – Emergency Mode Operation Plan; § 164.308(a)(7)(ii)(D) – Administrative Safeguards – Implementation Specifications – Testing and Revision Procedures; § 164.308(a)(7)(ii)(E) – Administrative Safeguards – Implementation Specifications – Applications and Data Criticality Analysis; § 164.316(a) – Standard – Policies and Procedures; and § 164.316(b) – Standard – Documentation.

Copies are retained by 4 weeks and then destroyed or recycled. (See Physical Safeguards – Device and Media Controls, page 88.)

NOTE: The practice will have to determine where to store the back up media. If you have two practice sites, consider storing the information at the second site. Perhaps you can store the information in a safe deposit box, or make arrangements to store it at one of your Business Associates, e.g., an attorney, accountant, or billing service. Make sure the backup is stored at a site where it is secure and protects the privacy of the information on the backup media.

The Security Officer or another workforce member authorized in writing by the Security Officer may retrieve the backup as required.

The practice does not store its medical records electronically [*or keeps paper copies of all medical records*]. Accordingly, the recovery of lost electronic-based PHI is not time-critical to patient care.

NOTE: If you keep medical records electronically, you will have to modify this language accordingly. In this case, recovery of electronic PHI may be critical to patient care.

Testing Restoration: Once a year, when critical new software is installed, and when new devices are installed, the practice checks to make sure it can recover lost data from its backup. Specifically, the practice reviews the back up files and compares them to the files on its computers. This is accomplished by comparing the size and dates of the files to ensure they are identical.

Disaster Recovery Plan: The practice does not store its medical records electronically [*or keeps paper copies of all medical records*]. Accordingly, the recovery of lost electronic-based PHI is not time-critical to patient care.

When a disaster has occurred – when electronic information is lost for whatever reason – the practice’s Security Officer implements the disaster recovery plan. The specific plan depends on the type and scope of the disaster:

- If PHI has been lost and the computer systems still function, the practice will attempt to restore the information from backup media.
- If PHI has been lost and some portion of the computer systems still function, the practice will attempt to restore the information from backup media to that portion of the computer system.
- If PHI has been lost and:
 - the computer systems still function, but the practice is unable to restore the information from backup media;
 - some portion of the computer systems still function, but the practice is unable to restore the information from backup media to that portion of the computer system;or

- the entire computer system has failed, the practice will obtain new computer equipment, install appropriate software, and restore the PHI in a timely fashion.

NOTE: If a practice has two locations, it may be able to restore the PHI at its second site. This would be an acceptable short-term solution.

NOTE: If a practice has electronic medical records and does not keep paper copies of those medical records, this section will have to be expanded. Restoration of the PHI becomes critical to the treatment of patients and must be accessible in a timely fashion.

Emergency Mode Operation: The practice does not need its electronic-based PHI to operate in emergency situations. All PHI needed in emergency situations is stored in paper format (paper medical records). Accordingly, the practice does not need any computer systems emergency mode operation plan.

NOTE: If a practice has electronic medical records and does not keep paper copies of those medical records, this section will have to be expanded. Restoration and emergency mode operation become critical to the treatment of patients and must be accessible in a timely fashion.

Education: The practice trains all workforce members regarding its contingency plans. The Security Officer is responsible for ensuring that back ups are made and stored offsite as required by these procedures.

NOTE: If a practice has electronic medical records and does not keep paper copies of those medical records, this section will have to be expanded. It will have to include more training to ensure that workforce members understand how to restore PHI and operate in emergency mode.

Administrative Safeguards – Physical Controls for Visitor Access

Background

One section of the Security Rule addresses physical controls for visitors.²⁸ In general, a covered entity – including a physician – must ensure that visitors do not have inappropriate or unauthorized access to PHI.

Model Policy

The practice ensures that visitors do not have inappropriate and unauthorized access to protected health information (PHI).

Model Procedures

The practice minimizes the presence of visitors in the office.

All visitors, including salespeople and pharmaceutical representatives, must sign in. Patients (and those accompanying patients) do not need to sign in as their presence is automatically documented by the practice.

If appropriate, the practice provides visitors an escort to ensure they do not have inappropriate or unauthorized access to PHI.

²⁸ § 164.310(a)(2)(iii) – Physical Safeguards – Implementation Specifications – Access Control and Validation Procedures.

Physical Safeguards

Numerous sections of the final Security Rule address physical safeguards.²⁹ The rule defines physical safeguards as “physical measures, policies and procedures to protect a covered entity’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.”

Small practices are required to implement appropriate policies and procedures to protect their protected health information (PHI) – confidential information – and ensure that it remains secure. Recall that the Security Rule only covers electronic information. The Privacy Rule also addresses confidential information kept in paper and other forms. In order to meet the Privacy Rule requirements, the practice also must protect paper-based information.

The following portions of this document address the physical safeguard policies and procedures that practices need to consider when implementing HIPAA privacy and security.

²⁹ § 164.304 – Definition – Physical safeguards; § 164.310 – Physical Safeguards; § 164.310(a)(1) – Standard – Facility Access Controls; § 164.310(a)(2)(i) – Contingency Operations; § 164.310(a)(2)(ii) – Facility Security Plan; § 164.310(a)(2)(iii) – Access Control and Validation Procedures; § 164.310(a)(2)(iv) – Maintenance Records; § 164.310(b) – Standard – Workstation Use; § 164.310(c) – Standard – Workstation Security; § 164.310(d)(1) – Standard – Device and Media Controls; § 164.310(d)(2)(i) – Implementation Specification – Disposal; § 164.310(d)(2)(ii) – Implementation Specification – Media Re-use; § 164.310(d)(2)(iii) – Implementation Specification – Accountability; and § 164.310(d)(2)(iv) – Implementation Specification – Data Backup and Storage.

Physical Safeguards – Access Control

Background

One key section of the Privacy Rule and numerous sections of the final Security Rule address access controls.³⁰ In general, a covered entity – including a physician – must have access control procedures to protect against unauthorized access to any PHI, whether paper or electronic.

Model Policy

The practice has appropriate access controls in place to ensure that only authorized persons have access to protected health information (PHI) on an appropriate basis.

Model Procedures

Facility Maintenance: The facility documents all facility repairs and modifications to the physical components of a facility, including maintenance, that impacts security, such as repairs to walls, adding or removing locks, doors, or hardware.

Personnel Security: The practice ensures that only authorized workforce members or business associates have access to PHI. All workforce members have access to PHI, as needed, to ensure the efficient operation of the practice. In addition, given the size and configuration of the practice, all workforce members have access to all computer terminals in the office, all programs on those computers, and all PHI used in those programs on an as needed basis. The practice assesses annually whether the duties of any workforce member have changed such that their current access is no longer appropriate.

NOTE: You will have to change this procedure if you limit access to computer programs or computers to specific personnel.

Termination: The practice terminates a workforce member's access to all PHI when the workforce member is terminated. The terminated workforce member is required to turn in any keys or other access devices that may have been issued by the practice, and all passwords are deactivated.

³⁰ § 164.530(c)(1) – Administrative Requirements – Standard – Safeguards; § 164.530(c)(2) Administrative Requirements – Implementation Specification – Safeguards; § 164.308(a)(1)(ii)(D) – Administrative Safeguards – Implementation Specifications – Risk Analysis – Information System Activity Review; § 164.308(a)(ii)(D)(3)(I) – Administrative Safeguards – Implementation Specifications – Standard: Workforce Security; § 164.308(a)(ii)(D)(3)(ii)(A) – Administrative Safeguards – Implementation Specifications – Authorization and/or Supervision; § 164.308(a)(ii)(D)(3)(ii)(B) – Administrative Safeguards – Implementation Specifications – Workforce Clearance Procedure; § 164.308(a)(ii)(D)(3)(ii)(C) – Administrative Safeguards – Implementation Specifications – Termination Procedures; § 164.308(a)(ii)(D)(4)(ii)(B) – Administrative Safeguards – Standard: Information Access Management – Implementation Specification: Access Authorization; § 164.308(a)(ii)(D)(3)(ii)(C) – Administrative Safeguards – Standard – Information Access Management – Access Establishment and Modification; § 164.312(a)(1) – Technical Safeguards – Standard – Access Control; § 164.312(d) – Technical Safeguards – Standard – Person or Entity Authentication; and § 164.312(e)(1) – Technical Safeguards – Standard – Transmission Security.

Physical Safeguards: The practice ensures that paper-based and electronic-media based PHI – PHI that is in physical formats and access to electronic-based PHI – is safeguarded.

Paper Records Management: The practice maintains paper medical and billing records. Each medical record and billing record contains PHI. The practice manages the medical records to ensure the privacy of the PHI in the medical records.

- Medical records are removed from the medical record files only for review by a workforce member for treatment, payment, or health care operations, to release records pursuant to an authorization, or as otherwise authorized by law.
 - When a medical record is removed from the medical record files for other than treatment, the medical record remains in the staff office and is not allowed to leave that area. When finished using the medical records, the record will be refiled.
 - When a medical record is removed from the medical record files for treatment purposes, the medical record either remains in the staff office (and is used and refiled) or is hand delivered by a workforce member to a physician’s office for review.
 - When a medical record is in a physician’s office, the medical record is kept behind the physician’s desk and away from the reach of any patient who may be in the physician’s office for a consultation. In addition, the medical record is kept in a folder so that any visitors to the physician’s office cannot see any PHI, including the patient’s name, which may reside on the cover of the medical record. When the physician is done using the medical record, it is hand delivered by a workforce member to the staff office for appropriate use and refileing.
- The practice places medical records in the door outside exam rooms when a patient is in the exam room awaiting the physician. The medical record is placed such that no PHI is visible to anyone walking by the exam room.
- When a physician and patient leave the exam room, the medical record is taken from the exam room and handed to another workforce member for processing and filing or placed in the physician’s office for further review.
- The medical records do not reside in cabinets that lock; however, the practice does lock the office at night, thereby securing the medical records.
- The doors to the practice are locked whenever the practice is closed and no one is present to monitor the practice and protect access to the medical records.

NOTE: If your medical records reside in locking cabinets, you will need to change these procedures. It is recommended that you have locking cabinets. In lieu of such cabinets, make sure the medical records room can be locked. You may have to lock the entire practice to secure the medical records. This is a minimally secure way of restricting access to your medical records.

NOTE: You need to review these procedures in detail to ensure they reflect your practice. Make whatever changes are necessary to ensure the procedures match your practice.

The practice manages the billing records to ensure the privacy of the PHI in the billing records.

- Billing records are removed from the billing record files only for review by a workforce member for payment, health care operations, or as otherwise allowed by law. In such cases, the billing record remains in the staff office and is not allowed to leave that area. When finished using the billing records, they will be refiled.
- The billing records reside in cabinets that do not lock; however, the office is locked at night.
- The doors to the practice are locked whenever the practice is closed and no one is present to monitor the practice and protect access to the billing records.

NOTE: If your billing records reside in locking cabinets, you will need to change these procedures. It is recommended that you have locking cabinets. In lieu of such cabinets, make sure the billing records room can be locked. You may have to lock the entire practice to secure the billing records. This is a minimally secure way of restricting access to your billing records.

NOTE: You need to review these procedures in detail to ensure they reflect your practice. Make whatever changes are necessary to ensure the procedures match your practice.

Posting of PHI: The practice does not post any PHI, including schedules, where it could be viewed by visitors or patients. Schedules and other PHI needed for the functioning of the practice is kept in places not accessible by patients and referred to as needed by workforce personnel.

Conversations Including PHI: The practice is careful to restrict conversations containing PHI.

- Conversations with a patient present occur in an exam room or a physician's office with the doors closed. Conversations in hallways or the reception area are avoided unless specifically initiated by the patient.
- Conversations in the hallway, especially near the reception area or other areas where patients may overhear the conversations, are avoided whenever possible.
- Workforce members, including a physician, do not take patient telephone calls in an exam room or in their office when another patient is present.
- The staff office is next to the reception area. Precautions are taken to minimize the PHI disclosed in telephone calls and other discussions that occur in the staff office. Whenever possible, those discussions occur in the back of the staff office farthest away from the reception area.

NOTE: This is a very sensitive portion of the regulations. Patients will be in the reception area and will be aware of conversations occurring in the staff office that they can overhear. You need to evaluate your practice to ensure that your office is organized in a manner that minimizes the release of PHI.

FAXes: The receipt and sending of FAXes is addressed under Physical Safeguards – Records Processing – Receiving, Sending, and Disposing of PHI, page 81.

Access to Computers: Access to computers is addressed under Administrative Safeguards – Physical Controls for Visitor Access, page 74, Physical Safeguards – Computer Workstation Use and Security, page 86, and Technical Safeguards – Personal or “Entity” Authentication, page 92.

Need-to-Know: The practice recognizes that each workforce member should have access only to the PHI they need to perform his or her particular job functions. Workforce members are not allowed access to PHI beyond the scope of their current job functions. This principle is closely related to the minimum necessary standards for use, disclosure, or request of PHI (see Uses and Disclosures – Minimum Necessary, page 61).

Uses of PHI: The practice has a very small workforce. Everyone in the office is responsible for every task from time to time. Accordingly, everyone in the office may have a need to review all PHI. The practice allows all members of its workforce to have access to all PHI, as necessary for them to carry out their job functions. The practice limits access to PHI to that information necessary for a member of its workforce to carry out his or her job functions. The amount and type of PHI necessary to carry out job functions varies depending on the specific tasks assigned to the member of the workforce each day depending on the needs of the practice.

Disclosures of PHI: The practice limits the PHI it discloses to that necessary to meet the purpose of the disclosure. For disclosures for:

- payment, the practice releases the information required to file a claim and, if requested, additional information requested by a health plan to adjudicate the claim (psychotherapy notes are not released without patient authorization for payment purposes); and
- health care operations, the practice releases the specific information required by the entity engaging in the health care operation, e.g., utilization review, quality assurance.

NOTE: The practice should list additional routine disclosures that it makes. For example, if the practice discloses information to a transcription service, accountant, or practice management company, it should specify the kinds of information disclosed.

The practice reviews such routine requests to ensure that they are reasonable and do not seek PHI beyond that reasonably required by the requestor to complete the purpose of the request. If, in the opinion of the practice, the requestor has requested more information than necessary, the practice so notifies the requestor and seeks clarification regarding what PHI they actually need.

The practice relies on a request for disclosure as being for the necessary amount of information if:

- the disclosure is to a public official and the public official represents that the request is for the minimum necessary information;
- the request is from another covered entity; or
- the request is from a business associate in order to provide a professional service to the practice and the professional represents that the request is for the minimum necessary information.

Requests for PHI: The practice sometimes has a need to request PHI from other entities, particularly other health care providers. In such instances, the practice will limit its request to that information that is “reasonably necessary” to accomplish the purpose of the request. For routine, recurring requests, the practice will describe the information being requested and purpose for the request.

Most often, the practice requests information related to the treatment of a patient. The minimum necessary requirements do not apply when the request is for purposes of treatment of a patient.

Use and Disclosure of Medical Record: The practice limits the use, disclosure, or request for a medical record to what is specifically needed in the professional judgment of the practice. For example, if there is a question regarding payment for a practice service, only the portion of the medical record related to that service is released.

The practice does not routinely use or disclose the entire medical record unless such use or disclosure is necessary, authorized by the patient, or allowed by law. If requested by a health care provider, the entire medical record will be made available to those involved in the treatment of the patient.

Physical Safeguards – Records Processing – Receiving, Sending, and Disposing of PHI

Background

One key section of the Privacy Rule and one section of the Security Rule address records processing.³¹ In general, a covered entity – including a physician – must ensure that PHI sent, received, or disposed of by the practice is secure.

Model Policy

The practice has procedures to ensure that protected health information (PHI) sent, received, and disposed of by the practice is secure.

Model Procedures

Receipt of PHI From Outside the Practice

The practice often receives PHI from outside the practice. PHI is received in three general formats: paper-based or electronic-media based (e.g., CD and diskette), FAX, and electronic transmission.

Paper-Based or Electronic Media-Based PHI: The practice often has PHI delivered to the practice in a physical format, e.g., paper records, CD, or diskette. When the practice receives such PHI, it immediately treats the PHI in the same manner as other PHI in the practice. Often the information is entered into the medical record, e.g., paper medical records and reports from other health care providers, or the practice's computer system, e.g., a remittance advice or explanation of benefits.

The practice handles the delivered PHI in the same manner as other PHI in the practice when the PHI is delivered via:

- the mail:
 - when the mail is initially reviewed and sorted
 - if the envelop indicates it contains confidential information or PHI; or
 - if the envelop is from a source that commonly sends PHI to the practice, e.g., a laboratory or health plan; or
 - when the mail is opened and read and it becomes clear it contains PHI;
- a delivery or messenger service:
 - when the practice initially receives and signs for or receives the letter or package
 - if the envelop indicates it contains confidential information of PHI; or

³¹ § 164.530(c)(1) – Administrative Requirements –Standard – Safeguards; § 164.530(c) – Administrative Requirements – Implementation Specification – Safeguards; and §164.312(e)(1) – Technical Safeguards – Transmission Security.

- if the envelope is from a source that commonly sends PHI to the practice, e.g., a laboratory or health plan; or
- when the letter or package is opened and read and it becomes clear it contains PHI; or
- a patient:
 - when the patient indicates the delivery includes PHI; or
 - when the practice reviews the delivery and becomes aware the delivery includes PHI.

FAXed PHI: The practice receives PHI via the FAX. The FAX machine is kept in the _____ area of the office. When the office is open, the FAX is monitored at all times by the practice’s workforce, and visitors are restricted from accessing the FAX machine. After hours, a FAX may be received. The same access controls apply to the FAX machine as apply to other paper-based records in the practice (see Physical Safeguards – Access Control, page 76).

Electronic PHI: The practice controls access to all computers through its policies and procedures, including Physical Safeguards – Access Control, page 76, Technical Safeguards – Personal or “Entity” Authentication, page 92, and Physical Safeguards – Device and Media Controls, page 88. Any PHI received electronically is sent to one of the practice’s computers and is secured in accordance with the practice’s policies and procedures governing electronic PHI as soon as it is received.

Sending PHI Outside the Practice

The practice sends PHI outside the practice. PHI is sent in two general formats: paper-based or electronic-media based (e.g., CD and diskette) and FAX.

Paper-Based or Electronic Media-Based PHI: The practice sends paper-based, or on occasion, electronic-media based PHI, outside the practice. The practice stamps all packages and envelopes containing such PHI as “**CONFIDENTIAL: PROTECTED HEALTH INFORMATION ENCLOSED**” or alternatively “**CONFIDENTIAL.**”

The practice charges fees equal to the actual cost of copying and mailing requested records. The practice determines the appropriate charge for providing the requested records and informs the requestor in advance of providing the records. If the requestor agrees to pay the fee in advance, the records will be provided. Otherwise, the records will not be provided unless the Privacy Officer determines that the charge is burdensome to the requestor. (See also Individual Rights – Inspect and Copy PHI, page 17.)

The packages and envelopes are sent:

- via mail [*for registered mail or return receipt only or deliver to addressee only*]; or
- via messenger or delivery service (e.g., United Parcel Service and FEDEX), deliver to addressee only.

FAXed PHI: The practice sends PHI via FAX, especially when the PHI is needed on a timely basis. Prior to sending PHI via FAX to a FAX number used on a regular basis, the practice initially confirms the FAX number as follows. The practice programs the FAX number into its

FAX machine. It then autodials the FAX number and sends a test FAX containing no PHI. Finally, the practice calls the location to which the FAX is being sent to confirm that the FAX was received.

For all other FAX numbers, the practice calls the location to which the PHI is being sent. The practice verifies the FAX number, that someone is present to receive the PHI, and that the PHI will be handled appropriately. The practice then sends the FAX. A FAX confirmation sheet is printed by the FAX machine and placed in the patient medical record.

FAXes are sent with a cover sheet. The cover sheet reads, in part:

IMPORTANT: THIS FAX IS INTENDED ONLY FOR THE INDIVIDUAL OR ENTITY TO WHICH IT IS ADDRESSED AND MAY CONTAIN INFORMATION THAT IS PRIVILEGED, CONFIDENTIAL, AND EXEMPT FROM DISCLOSURE UNDER APPLICABLE LAW. IF THE READER OF THIS MESSAGE IS NOT THE INTENDED RECIPIENT OR THE EMPLOYEE OR AGENT RESPONSIBLE FOR DELIVERING THE MESSAGE TO THE INTENDED RECIPIENT, YOU ARE HEREBY INFORMED THAT ANY USE, DISCLOSURE, DISTRIBUTION, OR COPYING OF THIS COMMUNICATION IS STRICTLY PROHIBITED. IF YOU HAVE RECEIVED THIS COMMUNICATION IN ERROR, PLEASE NOTIFY US IMMEDIATELY BY TELEPHONE AND RETURN THE ORIGINAL MESSAGE TO US AT THE ABOVE ADDRESS VIA THE UNITED STATE POSTAL SERVICE. THANK YOU.

NOTE: These model policies and procedures assume you are not sending PHI electronically, including confidential communications with your patients via e-mail. If you send PHI electronically via the Internet or using an "Intranet," additional procedures will need to be added to ensure the security of that PHI, including the appropriate encryption and/or password protection of the communications.

Disposal of PHI

The practice often has to dispose of PHI. Most often the PHI is in paper form and includes notes including telephone notes, duplicate copies of tests, and old medical records. The practice also has to dispose of PHI on electronic media, e.g., old computer file backups, and from time to time, the electronic PHI itself.

Record Retention: The practice recognizes the need to establish a record retention policy. SDSMA recommends the following minimum record retention policy (based upon state and federal law) as follows:

- 7 years after the last patient encounter for adult patients;
- 7 years after the last patient encounter for Medicare patients;
- indefinitely for childhood immunizations; and

- until the patient reaches the age of 20 for minor patients (under the age of 18).

South Dakota law provides that patient records may only be transferred to another practitioner, the patient, the patient's parents or personal representative, a licensed health care facility, or a corporation organized for the purpose of operating a health care clinic. If there is no one willing and able to accept the transfer of active patient records, the practitioner or his estate may retain or destroy them. However, the practitioner or his estate must make a reasonable attempt to give thirty days' prior written notice of the intent to destroy active records. State law also provides that the practitioner may destroy inactive patient records, or patient records if the practitioner is no longer aware of the patient's whereabouts.

Whether transferred by a retiring physician or the estate of a deceased physician, patient records are "protected health information," and therefore they may only be transferred consistent with the new federal rules. Accordingly, unless patient records are being transferred to another physician involved in the patient's care, they may not be transferred without the patient's authorization.

When attempting to notify a patient of the physician's intent to destroy records, the physician must make reasonable efforts to protect the privacy of the patient's protected health information, including the fact that the person was a patient. Accordingly, it is recommended that the practitioner comply with the State law notice requirement by first sending a generic letter asking the patient to contact the practitioner about an "important matter," but without being more specific. If the patient responds, the practitioner should then request written authorization to destroy the records. If there is no response, a more specific notice indicating that the records (other than those required by the new rules to be retained) will be destroyed may be sent.

NOTE: Many practices adopt a policy of 10 years after the last patient encounter as their record retention time period, in part because hospitals must retain records for 10 years. Any policy should not be less than the recommendations set forth above.

Paper-Based PHI: The practice disposes of paper-based or electronic media-based PHI as follows:

- Day-to-day paper containing PHI is not thrown out with the rest of the trash. It is collected and shredded by the practice. This includes telephone notes, draft letters, copies of memos, tests, and other items that no longer are needed, and information that is printed out for viewing and is maintained permanently electronically.

NOTE: If you intend to dispose of "day to day" paper in another manner, you must change this procedure accordingly. You may want to consider the use of locked "Shred-It" bins that can be emptied and shredded as needed. That avoids having to shred paper everyday.

- From time to time, the practice cleans out old medical records and other files that may contain PHI, but only in compliance with State law concerning the destruction of patient medical records. Such PHI is boxed and marked “**CONFIDENTIAL: CONTAINS PROTECTED HEALTH INFORMATION**” or simply “**CONFIDENTIAL.**” A company that shreds the PHI for the practice then picks it up. The shredding company is a Business Associate (see Uses and Disclosures – Business Associates, page 64) and maintains the privacy of the PHI until it is shredded and appropriately disposed of.

FAXed PHI: FAXed PHI is disposed of in the same manner as paper-based PHI.

Electronic or Electronic Media-Based PHI: The practice disposes of electronic PHI in a manner that ensures that no trace of the PHI remains and that the PHI cannot be restored using commonly available commercial programs (see Physical Safeguards – Device and Media Controls, page 88).

Physical Safeguards – Computer Workstation Use and Security

Background

Four sections of the Security Rule address computer workstations.³² In general, a covered entity – including a physician – must ensure that computer workstations are secure and cannot be used by unauthorized individuals or in an unauthorized manner.

Model Policy

The practice ensures that computer workstations and other devices are secure and protected and are used appropriately only by authorized individuals.

Model Procedures

The practice has a limited number of workforce members, and in general, each member is entitled to access all the protected health information (PHI) on each computer (see Uses and Disclosures – Minimum Necessary, page 61). When a workforce member logs onto a computer, they are entitled to view all the PHI accessible from that computer.

Each workforce member has his or her personal password, and computers have password-protected screen savers (see Technical Safeguards – Personal or “Entity” Authentication, page 92). Each workforce member logs off their computer when they are finished for the day or when they are away from their computer for longer than 1 hour.

The computers in the practice are located in _____. These locations are locked when the practice is closed. In addition, computers are secured at their locations using computer locks. Electronic media are protected in the same manner as paper-based PHI (see Physical Safeguards – Access Control, page 76).

The computer screens are positioned in such a manner as to minimize the ability of unauthorized individuals to view information on the screens. Individuals are not allowed in areas of the office where they will be able to view screens, except in passing.

NOTE: If the practice keeps PHI on mobile devices, you must include language regarding how you secure the PHI on those devices.

The practice protects PHI on mobile devices, including laptop computers, PDA’s, and cell phones.

³² § 164.304 – Definitions – Workstation; § 164.304 – Definitions – Security or Security Measures; § 164.310(b) – Standard – Workstation use; and § 164.310(c) – Standard – Workstation security.

- Laptop computers are logged in and out of the practice. The computers are password protected and the screen savers set to password protect the computers after 10 minutes of inactivity. Laptops also are backed up in a timely fashion (see Administrative Safeguards – Contingency Planning, page 69). The practice maintains the following laptops:
 - **LIST SPECIFIC LAPTOP**
 - **LIST SPECIFIC LAPTOP**

- PDA's commonly include patient schedule information and notes. The PDA's are password protected and synchronized with the computer workstations regularly to ensure timely backup (see Administrative Safeguards – Contingency Planning, page 69). The practice maintains the following PDA's:
 - **LIST SPECIFIC PDA**
 - **LIST SPECIFIC PDA**

- Cell phones contain phone numbers and, often, names of patients. They may also include text messaging, notes, and e-mail. Cell phones are password protected to limit inappropriate access. In addition, the call lists are periodically reviewed and unneeded telephone numbers deleted. The practice maintains the following cell phones:
 - **LIST SPECIFIC CELL PHONE**
 - **LIST SPECIFIC CELL PHONE**

NOTE: If the practice keeps PHI on other devices, such as testing equipment with electronic memory capabilities (including sonogram or audiology equipment), you must include language on how you secure these devices. *If these devices do not contain patient-identifying information, they do not contain PHI.*

The practice maintains PHI on a number of medical devices. The practice daily copies this information from the devices and places the information in the appropriate patient's medical record, and then deletes this information from the devices. In addition, the devices are locked up at night to ensure that they are not removed from the office. The practice maintains the following devices that contain or may contain PHI:

- **LIST SPECIFIC DEVICE**
- **LIST SPECIFIC DEVICE**

Physical Safeguards – Device and Media Controls

Background

Six sections of the Security Rule address device and media controls.³³ In general, a covered entity – including a physician – must ensure that PHI is appropriately protected when computer hardware (including electronic media, e.g., diskettes, tapes, CD's) and software are received, transported, or removed.

Model Policy

The practice ensures protected health information (PHI) is appropriately protected when computer hardware and software and computer devices are received by the practice, transported by the practice, moved within the practice, or removed from the practice.

Model Procedures

Accountability: The practice maintains a record of all computer hardware and electronic media that store PHI (see Device and Media Controls Log, page 90). This log indicates which workforce members are authorized to access PHI on each computer and electronic media and when the computer or media is removed from the practice location. This log is an integral part of the practice's risk assessment and ongoing evaluation. (See Administrative Safeguards – Risk Analysis, Risk Management, and Ongoing Risk Evaluation, page 68).

The practice records all devices and media that may contain PHI. This includes computers and related devices as well as other equipment, e.g., cell phones, personal digital assistants (PDA's), clinical devices that store patient-specific information, fax machines, and duplicating machines and printers that may store images.

Media Re-Use: Media may be reused only when all electronic PHI previously stored on the media is removed and unrecoverable. The practice only reuses media internally. Such media are always maintained securely and considered to contain PHI, even when they have been “cleaned.” This procedure is used due to the difficulty of completely destroying all traces of information on any electronic media to ensure that “cleaned” media cannot be recovered using a variety of techniques. Media are not “cleaned” for reuse and then sent out of the practice to be used by others. Rather, media are disposed of as discussed below.

Disposal of Devices and Media: The practice disposes of devices and media in a fashion that prevents the disclosure of PHI.

³³ § 164.103 – Definitions – Physical Safeguards, Electronic Media, and Facility; § 164.310(d)(1) – Physical Safeguards – Standard – Device and Media Controls; § 164.310(d)(2)(i) – Physical Safeguards – Implementation Specifications – Disposal; § 164.310(d)(2)(ii) – Physical Safeguards – Implementation Specifications – Media Reuse; § 164.310(d)(2)(iii) – Physical Safeguards – Implementation Specifications – Accountability; and § 164.310(d)(2)(iii) – Physical Safeguards – Implementation Specifications – Data backup and storage.

- **Devices:** PHI stored on devices is stored in a variety of different media. Computer information is stored on a hard drive and possibly diskettes, CD's, and DVD's. Cell phones, PDA's, and clinical devices also have storage devices that must be "cleaned" prior to disposal.
- **Media:** The practice stores information on diskettes, CD's, and DVD's. *The practice recognizes that simply deleting files does not remove the PHI from the media.*
 - Whenever possible, the practice overwrites the media completely using a commercially available program. The media is overwritten three times to ensure all PHI is destroyed. This includes data drives.
 - When data cannot be overwritten, e.g., on a CD or DVD that cannot be overwritten, the practice first makes a series of deep scratches on the media and then breaks the media in two pieces.

NOTE: If you do not store information on CD's or DVD's, you have to edit the above language. If you use other storage devices, e.g., memory sticks, Zip drives, and digital cameras, you will have to expand this language.

Data Backup and Storage: An important aspect of controlling PHI on devices and media is ensuring PHI is appropriately backed up and securely stored. In addition, it is vital to backup PHI prior to movement of equipment and media. Note that data backup also is addressed under Administrative Safeguards – Contingency Planning (page 69). Data backups are recorded as discussed under Contingency Planning.

Removal of Devices and Media: The practice may remove devices and media from the practice site, e.g., a portable computer or a PDA. In such instances, the practice will treat the device or media in the same fashion that it treats paper medical records. (See Physical Safeguards – Access Control, page 76.) Removed devices and media are documented on the Device and Media Controls Log, page 90.

Technical Safeguards

Numerous sections of the final Security Rule address technical safeguards.³⁴ The rule defines technical safeguards as “the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.”

Small practices are required to implement appropriate policies and procedures to protect their protected health information (PHI) – confidential information – and ensure that it remains secure. Recall that the Security Rule only covers electronic information. The Privacy Rule also addresses confidential information kept in paper and other forms. In order to meet the Privacy Rule requirements, the practice also must protect paper-based information.

The following portions of this document address the technical safeguard policies and procedures that practices need to consider when implementing HIPAA privacy and security.

³⁴ § 164.312 Technical Safeguards.

Technical Safeguards – Personal or “Entity” Authentication

Background

Five sections of the Security Rule address personal or entity authentication.³⁵ As used here, authentication is the means of establishing the validity of the identity of a user of the system. In general, a covered entity – including a physician – must have systems in place to ensure that only authorized users have access to PHI.

Model Policy

The practice ensures that only appropriate individuals can access protected health information (PHI) and has appropriate security mechanisms in place.

Model Procedures

Identification and Authentication: The practice issues each member of the workforce a unique user name and an initial password. Passwords must be changed at least once every 90 days. The Security Officer can override all workforce member passwords on an as needed basis and will ensure that new passwords are issued when such an override is necessary. The practice uses the standard password protection programs to access the computer and the programs in which it stores PHI, including Word, _____.

<p>NOTE: The practice should list the specific programs in which it stores PHI and password protects that information, including any practice management system, electronic health record, word processing, and data base management programs.</p>

Workforce members are educated regarding the appropriate choice of passwords (e.g., no names) and the need to keep passwords confidential. Workforce members do not keep passwords in written or electronic form in the practice and do not share passwords.

Automatic Logoff: The practice requires that all computers “lock up” and require an individual to sign on after a 15-minute period of not being used. Specifically, if a workforce member does not use his or her computer for 15 minutes, the system invokes a screen saver (so no one can view the information on the screen) and the workforce member has to reenter his or her password prior to continuing to work on the computer.

Another individual is not able to access the computer until the first individual reenters their password and then logs off the system.

³⁵ § 164.308(a)(5)(ii)(D) – Administrative Safeguards – Implementation Specifications – Password Management; § 164.312(a)(1) – Standard – Access Control; § 164.312(a)(2)(i) – Implementation Specification – Unique User Identification; § 164.312(a)(2)(iii) – Technical Specifications – Implementation Specifications – Automatic Logoff; and § 164.312(d) – Technical Specifications – Standard – Persons or Entity Authentication.

Password Deletion: The Security Officer deletes passwords when a workforce member is terminated or no longer has rights to access a particular system or computer.

Technical Safeguards – Security Configuration – Documentation, Testing, Inventory, Virus Control

Background

Three sections of the Security Rule address security configuration.³⁶ In general, a covered entity – including a physician – must have in place measures to ensure electronic-based PHI is not compromised as a result of software or hardware changes.

Model Policy

The practice has in place procedures to manage the integrity of its electronic-based protected health information (PHI) to ensure that system security is not compromised as a result of hardware or software changes.

Model Procedures

Documentation: The practice documents measures put in place to control access to data. This is addressed in other sections of these policies and procedures, including Physical Safeguards – Access Control, page 76, Technical Safeguards – Personal or “Entity” Authentication, page 92, and Physical Safeguards – Device and Media Controls, page 88.

Testing: The practice tests all hardware and software to ensure it meets the practice’s security policies and procedures. This testing occurs when the hardware or software is installed and not less often than once a year thereafter.

Inventory: The practice has in an inventory of all hardware and software used by the practice. This inventory lists each computer and its hardware configuration, as well as the software running on each computer. (See Device and Media Controls Log, page 90, and “PHI” Software Log, page 72.)

Virus Detection: The practice has in place a virus detection program to protect the practice’s data. The practice uses a commercially available program and updates it as recommended by the vendor. The practice runs a virus scan on each of its computers daily. The practice educates its workforce concerning virus protection, including how to prevent infections and the potential harm that can be caused by them, what to do if a virus is suspected, Trojan horse programs (password stealing), worms, and virus transport via various media types (e.g., diskettes and CD’s).

³⁶ § 164.308(a)(5)(ii)(B) – Administrative Safeguards – Implementation Specifications – Protection from Malicious Software; § 164.308(a)(7)(ii)(D) – Administrative Safeguards – Implementation Specifications – Testing and Revision Procedures; and § 164.316 – Policies and Procedures and Documentation Requirements.

Firewall: The practice has in place a firewall program to protect the practice's data. The practice uses a commercially available program and updates it as recommended by the vendor. The practice educates its workforce concerning the firewall and how to respond to firewall alerts to maximize protection of its computers.

Windows Update: The practice uses the Windows operating system. The practice checks at least once a week (every Monday morning) for critical updates by running the "Windows Update." Any critical updates are installed on all of the practice's computers. This helps to ensure that appropriate security "patches" are installed in a timely fashion.

NOTE: If the practice *does not use the Windows operating system*, then the previous paragraph needs to be changed to reflect how the practice's operating system is updated in accordance with the system vendor's recommendations.

Technical Safeguards – Audit Controls and Integrity

Background

Four sections of the Security Rule address audit controls and monitoring of internal system activity.³⁷ These provisions are complex to implement for small practices. In general, a covered entity – including a physician – must have in place measures to audit access to and use of protected health information to ensure that the PHI only is accessed and used appropriately and to ensure the integrity of the PHI.

Model Policy

The practice has in place procedures to audit access to and use of its protected health information (PHI) and to ensure the integrity of its electronic-based PHI.

Model Procedures

The practice audits use of its PHI – both paper and electronic. This is done through monitoring and controlling access to its computers and paper records as discussed above (see Physical Safeguards – Access Control, page 76, Administrative Safeguards – Physical Controls for Visitor Access, page 74, Physical Safeguards – Computer Workstation Use and Security, page 86, and Technical Safeguards – Personal or “Entity” Authentication, page 92). The practice also conducts periodic walkthroughs of its facility to ensure appropriate placement of FAX machines, medical records, and other PHI.

Given appropriate access controls, the PHI should not be changed inappropriately, thereby ensuring the integrity of the PHI. If the practice has any reason to believe the PHI has been inappropriately changed, the practice will compare the PHI to the latest backup (see Administrative Safeguards – Contingency Planning, page 69).

³⁷ § 164.308(a)(2)(D) – Administrative Safeguards – Implementation Specifications – Information System Activity Review; § 164.312(b) – Technical Safeguards – Standard – Audit Controls; § 164.312(c)(1) – Technical Safeguards – Standard – Integrity; and § 164.312(c)(2) – Technical Safeguards – Implementation Specifications – Mechanism to Authenticate Electronic Protected Health Information.

Technical Safeguards – Transmission Security

NOTE: The model policies and procedures included above assume that you are not sending or receiving PHI electronically, e.g., via e-mail, or over the Internet. If you do send any PHI electronically, the practice must ensure the “transmission security” of the PHI.

Please fill in the blanks and select the options below as appropriate.

Background

Three sections of the Security Rule address transmission security.³⁸ In general, a covered entity – including a physician – must have in place measures to ensure transmission security when PHI is electronically transmitted. Transmission security will ensure the integrity of PHI in transit.

Model Policy

The practice has in place procedures to secure protected health information (PHI) sent electronically.

Model Procedures

The practice uses [*program name*] to protect PHI sent electronically. Specifically, the practice locks all data files using [*a secure password*] and/or [*an encryption methodology*]. [*Passwords*] and/or [*encryption keys*] are sent to the receiving party in a separate secure transaction [*or are incorporated into the software or use public-private key encryption*].

³⁸ § 164.312(e)(1) – Standard – Transmission security; § 164.312(e)(2)(i) – Implementation specification – Integrity controls; and § 164.312(e)(1) – Implementation specification – Encryption.

Administrative Policies and Procedures

Administrative Requirements – Privacy Officer

Background

Two sections of the Privacy Rule address the need to appoint a Privacy Officer and a contact person for all issues related to the Privacy Rule.³⁹ In general, a covered entity – including a physician – is required to have a Privacy Officer and a contact person.

Model Policy

The practice has a Privacy Officer that serves as the contact person for all issues related to the Privacy Rule.

Model Procedure

The practice designates as its Privacy Officer **[FILL IN NAME OR TITLE OF PERSON]**. This person also serves as the practice's contact person for all issues related to the Privacy Rule, including, but not limited to:

- receiving complaints concerning the substance of the practice's privacy policies and procedures;
- receiving complaints concerning the practice's compliance with its privacy policies and procedures or more generally with the Privacy Rule requirements;
- providing further information about matters covered by the Notice of Privacy Practices; and
- receiving correspondence and requests related to the use or disclosure of protected health information (PHI) or individual rights.

Documentation

The practice keeps a written record of the names of each Privacy Officer. This information is maintained for a period of six years from the date of its creation.

³⁹§ 164.530(a) – Administration Requirements – Designation of a Privacy Official and Contact Person; and § 164.526(d)(1)(iv) – Administration Requirements – Amendment of Protected Health Information.

Administrative Requirements – Security Officer

Background

Three sections of the Security Rule address the need to appoint a Security Officer and a contact person for all issues related to the Security Rule.⁴⁰ In general, a covered entity – including a physician – is required to have a Security Officer and a contact person.

Model Policy

The practice has a Security Officer that serves as the contact person for all issues related to the Security Rule.

Model Procedure

The practice designates as its Security Officer **FILL IN NAME OR TITLE OF PERSON**. This person serves as the practice's contact person for all issues related to the Security Rule and works closely with the Privacy Officer.

<p>NOTE: The practice should consider whether the Privacy Officer and Security Officer should be the same person. In smaller practices this probably makes sense. Privacy issues will in many instances result from security breaches, and security breaches almost always result in privacy violations.</p>

Documentation

The practice keeps a written record of the names of each Security Officer. This information is maintained for a period of six years from the date of its creation.

⁴⁰§ 164.306 – Standard – General Rules – Maintenance; § 164.308(a)(2) – Standard – Assigned Security Responsibility; § 164.316(b) – Standard – Documentation.

Administrative Requirements – Changes in Law

Background

Two sections of the Privacy Rule address changes in law.⁴¹ In general, a covered entity – including a physician – is required to change the covered entity’s policies and procedures whenever a change in law necessitates such a change. In addition, the covered entity must promptly revise and distribute its Notice of Privacy Practices whenever there is a material change to the uses or disclosures of information, the individual’s rights, the covered entity’s legal duties, or other privacy practices stated in the notice. Keep in mind that the practice also must comply with all state and federal laws related to security.

Model Policy

The practice promptly makes any changes to its policies and procedures necessitated by changes in local, state, or federal law. In addition, the practice promptly revises and distributes its Notice of Privacy Practices whenever material changes are made with respect to the uses or disclosures of protected health information (PHI), the individual’s rights, the covered entity’s legal duties, or other privacy practices stated in the notice.

Model Procedure

When the practice becomes aware of changes in laws that necessitate changes in its privacy or security policies or procedures or changes in its Notice of Privacy Practices, the practice promptly makes and implements the changes. Except when required by law, a material change to the Notice of Privacy Practices is not implemented prior to the effective date of the notice in which the change is reflected.

The practice monitors changes in law through a variety of sources, including professional newsletters, journals, other publications and Web sites, its legal counsel, and the hospital medical staff.

⁴¹ § 164.530 (i)(3) – Changes in Law – Implementation Specification – Standard – Policies and Procedures; and § 164.520 (b)(3) – Revision to Notice – Implementation Specification – Content of Notice – Standard – Notice of Privacy Practices.

Administrative Requirements – Complaint Process

Background

Nine sections of the Privacy Rule address the complaint process.⁴² In general, a covered entity – including a physician – is required to have a process for individuals to file complaints with the covered entity and with the Secretary.

Model Policy

The practice allows all patients and their agents to file complaints with the practice and with the Secretary of the U.S. Department of Health and Human Services (DHHS).

Model Procedure

A patient or his or her agent may file a complaint with the practice whenever he or she believes that the practice has violated rights given under the Security or Privacy Rules.

Complaints made to the practice must be in writing, must describe the acts or omissions that are the subject of the complaint, and must be filed within 180 days of the time the patient became aware or should have become aware of the violation. Complaints must be addressed to the attention of the practice's Privacy Officer at the practice's address. Each complaint is entered into the practice's Complaint Log, page 103. The practice investigates each complaint and may, at its discretion, reply to the patient or the patient's agent.

Complaints to the Secretary of the U.S. Department of Health and Human Services must be in writing, must name the practice, must describe the acts or omissions that are the subject of the complaint, and must be filed within 180 days of the time the patient became aware or should have become aware of the violation. Complaints must be addressed to: Office for Civil Rights, U.S. Department of Health and Human Services, 1961 Stout Street - Room 1426, Denver, CO 80294, Phone - (303) 844-2024; TDD - (303) 844-3439, Telefax - (303) 844-2025. The practice will cooperate with the Secretary to investigate any complaints filed with the Secretary and allow the Secretary access to information requested by the Secretary.

The practice does not take any adverse action against any patient who files a complaint (either directly or through an agent) against the practice.

⁴² § 160.306 – Complaints to the Secretary; § 160.310(b) – Responsibilities of Covered Entities to Cooperate With Complaint Investigations and Compliance Review; § 160.312 – Secretarial Action Regarding Complaints and Compliance Reviews; § 164.530(a)(1)(ii) – Administrative Requirements – Standard – Personnel Designations; § 164.530(d) – Administrative Requirements – Standard – Complaints to the Covered Entity; § 164.530(g) – Administrative Requirements – Standard – Refraining from Intimidating or Retaliatory Action; § 164.520(B)(vi) – Notice of Privacy Practices – Complaints; § 164.524(d)(2)(iii) – Access of Individuals to Protected Health Information – Implementation Specifications – Denial of Access; and § 164.526(d)(iv) – Amendment of Protected Health Information – Implementation Specifications – Denial of Amendment.

Documentation

The practice will retain the documentation as required by § 164.530(j), including the written complaint and a record of their disposition. This information will be maintained for a period of six years from the date of its creation.

NOTE: This requirement may in some circumstances change the record retention periods for medical records under South Dakota law. See SDCL 36-4-37 and 36-4-38.

Administrative Requirements – Information Access Management

Background

Seven sections of the Security Rule address the requirement for information access management.⁴³ In general, a covered entity – including a physician – must: (1) authorize who can have access to what specific confidential information, system by system; (2) establish and modify access on an as needed basis; (3) supervise the workforce to ensure that only appropriate access is occurring; and (4) terminate access when required.

Model Policy

The practice only authorizes workforce members access to protected health information (PHI) on an as needed basis.

Model Procedure

Authorization: The practice authorizes all workforce members to have access to all PHI in the practice. The practice has a very small workforce. Everyone in the office is responsible for every task from time to time. Accordingly, everyone in the office has a need to review all PHI. The practice allows all members of its workforce to have access to all PHI, as necessary for them to carry out their job functions and support the efficient operation of the practice. The practice limits access to PHI to that information necessary for a member of its workforce to carry out his or her job functions. The amount and type of PHI necessary to carry out job functions varies depending on the specific tasks assigned to the member of the workforce each day depending on the needs of the practice. Access is only terminated when a workforce member leaves the practice.

Supervision: The Privacy Officer and the Security Office monitor the practice's operations to ensure that all workforce members are accessing PHI appropriately. Ongoing training and education about the need to access only that PHI required for each specific job task is a key part of the supervision.

Termination: As discussed under Physical Safeguards – Access Control, page 76, the practice terminates a workforce member's access to all PHI when the workforce member is terminated. The terminated workforce member is required to turn in any keys or other access devices that may have been issued by the practice and all passwords are deactivated.

⁴³ § 164.308(a) Standard – Workforce Security; § 164.308(a)(3)(ii)(A) – Implementation Specification – Authorization and/or Supervision; § 164.308(a)(3)(ii)(B) – Implementation Specification – Workforce Clearance Procedures; § 164.308(a)(ii)(C) Implementation Specification – Termination Procedures; § 164.308(a)(4)(i) Standard – Information Access Management; § 164.308(a)(4)(ii)(B) Implementation Specification – Access Authorization; and § 164.308(a)(4)(ii)(C) Implementation Specification – Access Establishment and Modification.

Administrative Requirements – Mitigation of Privacy Breaches

Background

One section of the Privacy Rule addresses the requirement for mitigation.⁴⁴ In general, a covered entity – including a physician – is required to take action to mitigate breaches in the use or disclosure of PHI. A breach occurs whenever PHI is used or disclosed in violation of the covered entity’s policies and or procedures.

In addition, a business associate must be terminated when possible after a material breach that has not been resolved. If the agreement cannot be terminated, then the practice must inform the Secretary of the situation.

Model Policy

The practice mitigates, to the extent practicable, any harmful effect that is known to the practice of a use or disclosure of protected health information (PHI) in violation of the practice’s policies and procedures, including uses and disclosures made by the practice’s business associates.

Model Procedure

The practice only acts to mitigate the harmful effects of a use or disclosure of PHI when

- the practice is aware of the use or disclosure;
- when the use or disclosure was made by the practice or any of its business associates; and
- when the use or disclosure is in violation of the practice’s privacy policies and procedures.

When the practice acts to mitigate the harmful effects of a use or disclosure, the practice takes measures to the extent practicable. The practice takes reasonable steps based on where the information has been disclosed, how it might be used to cause harm to the patient or another individual, and what steps can actually have a mitigating effect.

Documentation

The practice documents all uses and disclosures of PHI in violation of the practice’s policies and procedures on its Mitigation Log, page 106. The practice also documents the reasonable actions taken to mitigate the harm created by those uses and disclosures. The practice’s Privacy Officer maintains this documentation. This information is maintained for a period of six years from the date of its creation.

⁴⁴ § 164.530(f) – Administrative Requirements – Mitigation.

Mitigation Log

Patient Name	Date Aware of Problem	Description of Problem/Mitigation Efforts Taken, If Any	Date Problem Evaluated	Date Mitigation Taken

Administrative Requirements – Security Incident Procedures

Background

Six sections of the Security Rule address security incident procedures.⁴⁵ In general, a covered entity – including a physician – must record and address security incidents – “the attempted or successful unauthorized access, use, disclosure, modification, or destruction” of electronic protected health information.

Model Policy

The practice monitors, records, and responds to all security incidents in a timely fashion.

Model Procedures

The practice monitors information system activity to detect security incidents – “the attempted or successful unauthorized access, use, disclosure, modification, or destruction” of electronic protected health information. The practice records and follows up when it determines: someone or some program has entered its computer system from outside the practice, e.g., a virus or worm, or someone inside the practice accesses, uses, or changes PHI in an unauthorized manner.

In the event of a security incident, the practice documents the occurrence on the Security Incident Log, page 108. The Security Officer determines if there have been any harmful effects as a result of the incident. If there have been harmful effects, the Security Officer takes steps to mitigate those harmful effects.

If specific individual PHI has been disclosed, the Privacy Officer records this information on the Mitigation Log and the practice’s mitigation procedures followed (see Administrative Requirements – Mitigation of Privacy Breaches, page 105).

The practice trains the workforce to deal with security incidents and minimize harmful effects of security incidents.

NOTE: A “virus” is computer code that can damage your software, hardware, or files and is designed to travel from computer to computer. A “worm” is like a virus, but it travels from computer to computer on its own by using e-mail or a similar system.

⁴⁵ § 164.304 – Definition of Security Incident; § 164.308(a)(1)(ii)(D) – Implementation Specification – Security Incident Tracking Reports as a Part of Information System Activity Review; § 164.308(a)(6)(i) – Standard – Security Incident Procedures; § 164.308(a)(6)(ii) – Implementation Specification – Response and Reporting; § 164.314(a)(2)(i)(C) – Implementation Specification – Obligation of Business Associates, Created by Business Associate Contracts, to Report Security Incidents to Covered Entities; and § 164.314(a)(2)(iv) – Implementation Specification – Obligation of Plan Sponsors, Created by Plan Document Amendment, to Report Security Incidents to the Group Health Plan.

Administrative Requirements – Whistleblowers/Crime Victims

Background

Two sections of the Privacy Rule address whistleblowers and the reporting of violations.⁴⁶ In general, a covered entity – including a physician – is required to use and disclose PHI in whistleblower and crime victim cases without an authorization.

Model Policy

The practice allows the use and disclosure of protected health information (PHI) in the case of a whistleblower acting in good faith or when a workforce member is a victim of a criminal act.

Model Procedure

Whistleblowers: The practice allows a workforce member or business associate to use or disclose PHI, provided the workforce member or business associate believes in good faith that the practice has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the practice potentially endangers one or more patients, workers, or the public. The disclosure must be made to the proper agency including:

- a health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the practice;
- an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the practice; or
- an attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in the previous paragraph.

Victim of a Crime: The practice allows a workforce member who is the victim of a criminal act to use or disclose PHI to a law enforcement official, provided that:

- the PHI disclosed is about the suspected perpetrator of the criminal act; and
- the PHI disclosed is limited to name, address, date and place of birth, social security number, ABO blood type and Rh factor, type of injury, date and time of treatment, date and time of death, and other distinguishing physical characteristics.

Workforce Education: The practice educates its workforce regarding the whistleblower and crime victim provisions. The practice makes it clear that the right of workforce members to

⁴⁶ § 164.502(j) – Standard – Disclosures by Whistleblowers and Workforce Member Crime Victims; and § 164.512(f)(2)(i) – Listing of the Protected Health Information that May Be Disclosed by a Workforce Member Who is a Victim of a Crime.

disclose PHI is limited. Workforce education includes methods by which violations can be reported. This includes:

- reporting violations to an immediate supervisor;
- reporting violations to the practice's Compliance Officer who also is the practice's Privacy Officer; and
- reporting violations through hotlines established specifically for the purpose of reporting violations.

Workforce members are informed that:

- they are obligated by law to report such violations;
- no retribution or retaliation for reporting violations will occur, so long as reporting is done in good faith; and
- anyone who deliberately makes a false accusation with the purpose of harming or causing retaliation against another workforce member will be subject to discipline, up to and including dismissal.

Administrative Requirements – Awareness and Training For Staff

Background

One section of the Privacy Rule and five sections of the Security Rule address the requirements for training staff.⁴⁷ In general, a covered entity – including a physician – is required to ensure its workforce is trained with respect to the covered entity’s privacy and related security policies and procedures. All workforce members who have access to PHI in any way must be trained.

Model Policy

The practice trains its workforce on all aspects of its privacy and related security policies and procedures.

Model Procedure

The practice provides training to its workforce with respect to the privacy and security of protected health information (PHI). Specifically, the practice:

- provided each member of its workforce initial training no later than April 14, 2003, or within the first 30 days of work at the practice, if that date is on or after April 14, 2003;
- provides additional training to each member of its workforce when there is a material change in the practice’s policies and procedures prior to the effective date of those changes (unless the change is required by law and occurs prior to changes being made to the policies and procedures, in which case the training occurs as soon as possible after the practice becomes aware of the required change);
- documents on its Training Log that the training has been provided; and
- requires each workforce member to sign a statement (attached) that the workforce member has been trained and understands the practice’s policies and procedures regarding PHI.

The practice initially educates workforce members by reviewing the practice’s privacy and related security policies and procedures as contained in this document, including protection from malicious software (see Technical Safeguards – Security Configuration – Documentation, Testing, Inventory, Virus Control, page 94) and proper use of passwords (see Technical Safeguards – Personal or “Entity” Authentication page 92). The Privacy Officer and Security Officer then work with each workforce member to ensure they are implementing the policies and procedures as required.

⁴⁷ § 164.308(a)(5)(ii)(A) – Implementation Specification – Security Reminders; § 164.308(a)(5)(ii)(B) – Implementation Specification – Protection from Malicious Software; § 164.308(a)(5)(ii)(C) – Implementation Specification – Log-in Monitoring; § 164.308(a)(5)(ii)(D) – Implementation Specification – Password Management; § 164.530 (b) – Administrative Requirements – Standard – Training; and § 164.308(a)(5)(i) – Administrative Safeguards – Standard – Security Awareness and Training.

The practice provides periodic education to workforce members. At least once a year, or whenever specific issues are identified, the practice provides additional training to ensure that all workforce members follow the practice's privacy and security policies and procedures. In addition, the practice reviews specific privacy and security issues at its monthly staff meetings.

Documentation

The practice documents all workforce training on its Training Log, page 113. The practice records the date of the training, the workforce members trained, and the material covered in the training session. The practice also requires each workforce member to sign a statement that they have been trained and understand the practice's policies and procedures (see Model Acknowledgment of Training, page 114). The practice maintains this information for a period of six years from the date of its creation.

Model Acknowledgment of Training

(ON PRACTICE LETTERHEAD)

I, _____, acknowledge that I have been trained in the Health Insurance
(Print name of Workforce Member)

Portability and Accountability Act (HIPAA) privacy and security policies and procedures of
[NAME OF THE PRACTICE]. I understand that I must keep private and secure the protected
health information of the practice.

I understand and agree to adhere to all of these policies and procedures. Further, I
understand that I am subject to sanctions, up to and including termination, for violation of the
practice's policies and procedures.

Signature: _____ Date: _____

Administrative Requirements – Workforce Sanctions

Background

Six sections of the Privacy Rule and one section of the Security Rule address sanctions against members of a covered entity's workforce.⁴⁸ In general, a covered entity – including a physician – is required to sanction members of its workforce who do not comply with the covered entity's policies and procedures.

Model Policy

The practice sanctions workforce members who use or disclose protected health information (PHI) in violation of the practice's policies and procedures.

Model Procedure

The practice applies appropriate sanctions against workforce members who fail to comply with the practice's privacy and security policies and procedures. The particular sanction depends on the harm created by the unauthorized use or disclosure of PHI, whether the use or disclosure was intentional or unintentional, and whether or not the workforce member has previously used or disclosed PHI in violation of the practice's privacy policies and procedures.

Generally sanctions will be imposed as follows:

- For *an initial violation* by a member of the practice's workforce of the practice's policies and procedures that occurs:
 - *unintentionally*, the workforce member receives a warning. In addition, the practice requires the workforce member clearly to understand how the unintentional use or disclosure occurred and how to avoid future such uses or disclosures.
 - *intentionally* and causes:
 - *no or minimal harm* to the subject of the PHI or to other individuals, the workforce member receives a warning. In addition, the practice requires the workforce member clearly to understand the need not to use or disclose PHI in violation of the practice's policies and procedures.
 - *significant harm* to the subject of the PHI or to other individuals, the workforce member is given time off without pay. The amount of time off will range from 1 to 3 days and will depend on the harm caused. In addition, the practice requires the workforce member clearly to understand the need not to use or disclose PHI in violation of the practice's policies and procedures.

⁴⁸§ 164.308(a)(3)(ii)(C) – Implementation Specification – Termination Procedures; § 164.502(j)(1) – Disclosures by Whistleblowers; § 164.502(j)(2) – Disclosures by Workforce Members who are Victims of a Crime; § 164.530(e)(1) – Standard – Sanctions; § 164.530(e)(2) – Implementation Specifications – Documentation; § 164.530(g) – Standard – Refraining from Intimidating or Retaliatory Acts; and § 164.530(j) – Standard – Documentation.

- For a *repeat violation* by a member of the practice's workforce of the practice's policies and procedures that occurs:
 - *unintentionally*, the workforce member will receive time off without pay. The time off will range from 1 to 3 days and will depend on how much harm, if any, was caused to the subject of the PHI or to other individuals. In addition, the practice requires the workforce member clearly to understand how the unintentional use or disclosure occurred and how to avoid future such uses or disclosures.
 - *intentionally* and causes:
 - *no or minimal harm* to the subject of the PHI or to other individuals, the workforce member receives time off without pay. The time off will range from 3 to 5 days and will depend on how much PHI was used or disclosed and for what purpose. In addition, the practice requires the workforce member clearly to understand the need not to use or disclose PHI in violation of the practice's policies and procedures.
 - *significant harm* to the subject of the PHI or to other individuals, the workforce member is given time off without pay. The amount of time off will range from 3-7 days depending on how much harm was caused to the subject of the PHI or to other individuals. In addition, the practice requires the workforce member clearly to understand the need not to use or disclose PHI in violation of the practice's policies and procedures.
- If a workforce member intentionally uses or discloses PHI four or more times, the workforce member will be terminated.

Exceptions to Applying Sanctions to Workforce Members

There are three exceptions to workforce sanctions: the whistleblower exception, the crime victim exception, and the complaints, investigations, and opposition exception.

Whistleblower Exception: The practice will not impose sanctions against a workforce member for the use or disclosure of PHI made in accordance with the whistleblower provisions (see Administrative Requirements – Whistleblowers/Crime Victims, page 109).

Crime Victim Exception: The practice will not impose sanctions against a workforce member for the use or disclosure of PHI made in accordance with the crime victim provisions (see Administrative Requirements – Whistleblowers/Crime Victims, page 109).

Complaints, Investigations, and Opposition Exceptions: The practice does not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against workforce members and others who:

- file a complaint with the Secretary of DHHS;
- testify, assist, or participate in an investigation, compliance review, proceeding, or hearing under Part C of Title XI – utilization and peer review programs for Medicare and Medicaid; or
- oppose any act or practice made unlawful by the Privacy Rules, provided the workforce member or business associate has a good faith belief that the practice is unlawful and the manner of the opposition is reasonable and does not involve disclosure of PHI.

Documentation

The practice will document all sanctions taken against workforce members in its personnel files. The practice maintains this information for a period of six years from the date of its creation.

Administrative Requirements – Documentation

Background

Eight sections of the Privacy Rule and five sections of the Security Rule address the need for documentation.⁴⁹ In general, a covered entity – including a physician – is required to document when PHI is released for other than payment, treatment, or health care operations, when an individual makes a request of the practice and the response of the practice, a disclosure is made pursuant to an authorization, and when information is used for research purposes.

Model Policy

The practice maintains all documentation as required by the Privacy and Security Rules and discussed throughout this policy and procedures manual.

Model Procedure

Document Retention: All documentation is maintained for a minimum period of seven years. (See page ___ concerning Records Retention).

Documentation of Individual Rights Provisions

Notification: The practice maintains copies of each version of its Notice of Privacy Practices and documents that it has provided its Notice to every direct treatment patient (see page 7).

Tracking and Accounting for Uses and Disclosures of PHI: The practice documents all uses and disclosures of PHI and all requests for accountings of disclosures as required in the Privacy Rule (see Disclosures of PHI Tracking Log, page 15, and Requests for Accounting of Disclosures Log, page 16).

Inspection and Copying of PHI: The practice documents requests for inspection and copying of PHI and responses to those requests (see Inspection and Copying Request Log, page 21).

Amendment of PHI: The practice documents requests for amendments to PHI and responses to those requests (see Amendment Request Log, page 28).

⁴⁹ § 164.316(a) – Standard – Policies and Procedures; § 164.314(b) – Standard – Documentation; § 164.316(b)(2)(i) – Implementation specification – Time Limits; § 164.316(b)(2)(ii) – Implementation specification – Availability; § 164.316(b)(2)(iii) – Implementation specification – Updates; § 164.508 – Uses and Disclosures for which an Authorization is Required; § 164.512(i) – Uses and Disclosures for Research Purposes – Documentation Requirements of IRB; § 164.520(e) – Notice of Privacy Practices for Protected Health Information – Implementation Specifications – Documentation; § 164.522 – Rights to Request Privacy Protection for Protected Health Information; § 164.524(e) – Access of Individuals to Protected Health Information – Implementation Specification – Documentation; § 164.526(f) – Amendment of Protected Health Information – Implementation Specification – Documentation; § 164.528(d) – Accounting of Disclosures of Protected Health Information – Implementation Specification: Documentation; and § 164.530(j) – Administrative Requirements – Standard – Documentation.

Confidential Communications: The practice documents requests for confidential communications and responses to those requests (see Request for Confidential Communications Log, page 34).

Restriction of Use of PHI: The practice documents all requests for restrictions of the use of PHI for treatment, payment, or health care operations and responses to those requests (see Disclosure Restriction Log, page 37).

Authorizations: The practice maintains copies of all authorizations (see **Model Authorization Form for Release of Confidential Health Information**, page 42).

Documentation of Security Requirements

Risk Analysis: The practice has completed a risk analysis (see Small Practice Security Risk Analysis, page 128).

Evaluation: The practice updates its risk analysis on an annual basis (see Administrative Safeguards – Risk Analysis, Risk Management, and Ongoing Risk Evaluation, page 68).

PHI Software Log: The practice maintains a log of all software containing or using PHI (see “PHI” Software Log, page 72).

PHI Backup Log: The practice maintains a log of all its PHI data backups (see Backup Log, page 73).

Device and Media Controls Log: The practice keeps a log of all computer devices and electronic media (see Device and Media Controls Log, page 90).

Documentation of Administrative Requirements

Privacy Officer: The practice documents the name and title of its Privacy Officer (see page 98).

Security Officer: The practice documents the name and title of its Security Officer (see page 99).

Complaints: The practice documents all complaints and the resolution of those complaints (see Complaint Log, page 103).

Mitigation: The practice documents all known violations of its privacy policies and procedures and the actions taken to mitigate any harm caused by those violations (see Mitigation Log, page 106).

Security Incidents: The practice documents all security incidents (see Security Incident Log, page 108).

Training: The practice documents the training provided to each workforce member (see Training Log, page 113).

Workforce Sanctions: The practice documents all sanctions it takes against workforce members (see page 117).

HIPAA Privacy and Security Readiness Checklist

POLICIES AND PROCEDURES						
Topic	Policy Developed	Procedure Developed	Procedure Tested	Need to Modify?	Policy Finalized	Procedure Finalized
PRIVACY – INDIVIDUAL RIGHTS						
Notice of Privacy Practices				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Accounting for Disclosures of PHI				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Inspect and Copy PHI				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Request Amendment to PHI				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Request Confidential Communications				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Request Restriction of Disclosures				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Authorizations				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Waiver of Rights				<input type="checkbox"/> Yes <input type="checkbox"/> No		

POLICIES AND PROCEDURES

Topic	Policy Developed	Procedure Developed	Procedure Tested	Need to Modify?	Policy Finalized	Procedure Finalized
PRIVACY – USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION						
Verification of Identity				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Personal Representatives				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Disclosure to Those Involved in Individual's Care				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Uses and Disclosures Required by Law				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Uses and Disclosures in Emergency Situations				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Marketing Purposes				<input type="checkbox"/> Yes <input type="checkbox"/> No		
De-identification of PHI				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Deceased Individual's PHI				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Research Activities				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Other Uses and Disclosures That Do Not Apply to Practice				<input type="checkbox"/> Yes <input type="checkbox"/> No		

POLICIES AND PROCEDURES

Topic	Policy Developed	Procedure Developed	Procedure Tested	Need to Modify?	Policy Finalized	Procedure Finalized
Minimum Necessary				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Business Associates				<input type="checkbox"/> Yes <input type="checkbox"/> No		
SECURITY – ADMINISTRATIVE SAFEGUARDS						
Risk Analysis, Risk Management, and Ongoing Risk Evaluation				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Contingency Planning				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Physical Controls for Visitor Access				<input type="checkbox"/> Yes <input type="checkbox"/> No		
SECURITY – PHYSICAL SAFEGUARDS						
Access Control				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Records Processing – Receiving, Sending, and Disposing of PHI				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Computer Workstation Use and Security				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Device and Media Controls				<input type="checkbox"/> Yes <input type="checkbox"/> No		

POLICIES AND PROCEDURES

Topic	Policy Developed	Procedure Developed	Procedure Tested	Need to Modify?	Policy Finalized	Procedure Finalized
-------	------------------	---------------------	------------------	-----------------	------------------	---------------------

SECURITY – TECHNICAL SAFEGUARDS

Personal or “Entity” Authentication				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Security Configuration – Documentation, Testing, Inventory, Virus Control				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Audit Controls and Integrity				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Transmission Security				<input type="checkbox"/> Yes <input type="checkbox"/> No		

PRIVACY AND SECURITY ADMINISTRATIVE REQUIREMENTS

Privacy Officer				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Security Officer				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Changes in Law				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Complaint Process				<input type="checkbox"/> Yes <input type="checkbox"/> No		

POLICIES AND PROCEDURES

Topic	Policy Developed	Procedure Developed	Procedure Tested	Need to Modify?	Policy Finalized	Procedure Finalized
Information Access Management				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Mitigation of Privacy Breaches				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Security Incident Procedures				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Whistleblowers/Crime Victims				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Awareness and Training for Staff				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Workforce Sanctions				<input type="checkbox"/> Yes <input type="checkbox"/> No		
Documentation				<input type="checkbox"/> Yes <input type="checkbox"/> No		

RECOMMENDED TRACKING LOGS

	Developed	Incorporated into Procedures
Disclosures of PHI Tracking Log		
Requests for Accounting of Disclosures Log		
Inspection and Copying Request Log		
Amendment Request Log		
Request for Confidential Communication Log		
Disclosure Restriction Log		
“PHI” Software Log		
Backup Log		
Device and Media Controls Log		
Complaint Log		
Mitigation Log		
Security Incident Log		
Training Log		

OTHER FORMS AND DOCUMENTS

	Developed	Incorporated into Procedures
Notice of Privacy Practices		
Receipt of Notice of Privacy Practices Form		
Consent for Release and Use of PHI and Receipt of Notice of Privacy Practices Form (Optional)		
Request for Medical Records Acceptance Form Letter		
Request for Inspection or Copying of Confidential Information Denial Form Letter		
Acceptance of Request to Amend Medical or Billing Records Form Letter		
Denial of Request to Amend Medical or Billing Records Form Letter		
Request for Confidential Communication		
Authorization Form for Release of Confidential Health Information		
Acknowledgment of Training Form		

Small Practice Security Risk Analysis



This risk analysis follows the ISMS and ISMIE Mutual Insurance Company Model Security Policies and Procedures. If you answer “YES” to all the questions in this risk analysis, then your practice is on the way to meeting the HIPAA Security Rule requirements as reflected in those model policies and procedures. *The policies and procedures list more specific implementation specifications and need to be reviewed in detail to ensure that they reflect the actual procedures in your office.* Keep in mind that some items may appear in several places in the model policies and procedures. In most instances, those items are addressed only once in this risk analysis.

If you answer “NO” to any of the questions in the risk analysis, you need to evaluate your practice to determine if you need to alter your current policies and procedures to ensure compliance with the HIPAA Security Rule. In addition, the model policies and procedures will need to be modified if you decide that it is reasonable for your practice to answer “NO” to any of the questions.

Please file your completed risk analysis with your other HIPAA documentation. This is an important piece in documenting that you are complying with the HIPAA Security Rule.

This risk analysis should be reviewed and updated once a year or more frequently as required by your policies and procedures.

Administrative Safeguards			
Contingency Planning			
	“Criticality” Analysis: Does the practice keep a log of its devices and media and a log of the software on each of its devices that may contain confidential information? <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> NOTE: If a practice has electronic medical records and does not keep paper copies of those medical records, this section will have to be expanded. The analysis will have to document which systems are necessary – critical – to ensure timely patient care. </div>	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Data Backup Plan		
	Does the practice backup all protected health information (PHI) – confidential information – maintained on its computer systems on at least a weekly basis?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Is the backup password protected?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Are two copies made and one stored at a secure off-site location?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Are backups logged?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	

	Are copies retained for four weeks and then destroyed or recycled?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Is the Security Officer or another authorized workforce member able to retrieve the backup as required?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Testing Restoration: Once every six months, when new software is installed, and when new devices are installed, does the practice check to make sure it can recover lost data from its backup?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Disaster Recovery Plan			
	Does the practice have a disaster recovery plan that depends on the type and scope of the disaster, e.g., PHI has been lost and the computer systems still function or only some portion of the computer systems still function?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	When a disaster has occurred – when electronic information is lost for whatever reason – does the practice’s Security Officer implement the disaster recovery plan?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	NOTE: If a practice has electronic medical records and does not keep paper copies of those medical records, this section will have to be expanded. Restoration of PHI becomes critical to the treatment of patients and must be accessible in a timely fashion.		
	Emergency Mode Operation: The practice does not need its electronic-based PHI to operate in emergency situations.	Not Applicable	
	NOTE: If a practice has electronic medical records and does not keep paper copies of those medical records, this section will have to be expanded. Restoration and emergency mode operation become critical to the treatment of patients and must be accessible in a timely fashion.		
Physical Controls for Visitor Access			
	Does the practice minimize the presence of visitors in the office?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Does the practice require all visitors (not patients) to sign in?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	If appropriate, does the practice provide visitors an escort to ensure they do not have inappropriate or unauthorized access to PHI?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

Physical Safeguards			
Access Control			
Personnel Security			
	Does the practice ensure that only authorized workforce members have access to PHI?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Given the size and configuration of the practice, do all workforce members have access to all computer terminals in the office, all programs on those computers, and all PHI used in those programs on an as needed basis?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Termination			
	Does the practice terminate a workforce member’s access to all PHI when the workforce member is terminated?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Does the practice require the terminated workforce member to turn in any keys or other access devices that may have been issued by the practice?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

	Does the practice deactivate all passwords of the terminated workforce member?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
--	--	------------------------------	-----------------------------

Physical Safeguards			
	Does the practice ensure that paper-based and electronic-media based PHI are safeguarded?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Does the practice manage medical records to ensure the privacy of the PHI in the medical records?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Does the practice manage the billing records to ensure the privacy of the PHI in the billing records?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Is the practice careful not to post any PHI, including schedules?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Is the practice careful to restrict conversations containing PHI?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Need-to-Know			
	Does the practice recognize that each workforce member only has access to the PHI he or she needs to perform his or her particular job functions?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Does the practice limit the PHI it discloses to that necessary to meet the purpose of the disclosure, including for payment and health care operations?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Does the practice limit its requests for PHI to information that is “reasonably necessary” to accomplish the purpose of the request, and for routine, recurring requests, have in place a description of the information being requested and the purpose for the request?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Records Processing – Receiving, Sending, and Disposing of PHI			
Receiving PHI			
	Does the practice handle PHI delivered from outside the practice (electronic media or paper records) in the same manner as other PHI in the practice when the PHI is delivered via the mail or by a patient?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	If the practice receives PHI via fax, is the fax machine kept in a secure area of the office?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	When the office is open, is the fax monitored at all times by the practice’s workforce and are visitors restricted from accessing the fax machine?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Is any PHI received electronically sent to one of the practice’s computers and secured in accordance with the practice’s policies and procedures governing electronic PHI?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Sending PHI			
	When the practice sends PHI outside the practice, does it stamp all packages and envelopes containing such PHI as “ CONFIDENTIAL: PROTECTED HEALTH INFORMATION ENCLOSED ” or simply “ CONFIDENTIAL ”?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Prior to sending PHI via fax to a fax number used on a regular basis, does the practice initially confirm the fax number by actually sending a fax and confirming its receipt?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Are all faxes sent with a cover sheet that indicates the confidential nature of the fax and how to proceed if the fax was received in error?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Disposal of Paper-Based PHI: Does the practice collect and shred paper-based PHI, including telephone notes, draft letters, copies of memos, tests, and other items that no longer are needed, and information that is printed out for viewing and is maintained permanently electronically?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

Computer Workstation Use and Security

Does each workforce member have his or her personal password?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Do the practice's computers have password-protected screen savers?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Does each workforce member log off his or her computer when he or she is finished for the day or when away from their computer for longer than one hour?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Are the locations that contain the computers locked when the practice is closed?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Are the computers secured at their locations using computer locks?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Are electronic media protected in the same manner as paper-based PHI?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Are the computer screens positioned in such a manner as to minimize the ability of unauthorized individuals to view information on the screens?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Are individuals not allowed in areas of the office where they will be able to view screens, except in passing?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
<p>NOTE: If the practice keeps PHI on mobile devices, you must include language regarding how you secure the PHI on those devices.</p> <p>Does the practice protect PHI on mobile devices, including laptop computers, personal digital assistants (PDA's) and cell phones?</p> <p>NOTE: If the practice keeps PHI on other devices, such as testing equipment, you must include language on how you secure these devices. <i>If these devices do not contain patient-identifying information, they do not contain PHI.</i></p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No

Device and Media Controls

Accountability		
Does the practice maintain a record of all computer hardware and electronic media that store PHI, and does this log indicate (1) which workforce members are authorized to access PHI on each computer and electronic media and (2) when the computer or media is removed from the practice location?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Does the practice record all devices and media that may contain PHI, including computers and related devices, as well as other equipment, e.g., cell phones, PDA's, clinical devices that store patient-specific information, fax machines, and duplicating machines and printers that may store images?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Media Re-Use: Does the practice reuse media only when all electronic PHI previously stored on the media is removed and unrecoverable?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Disposal of Devices and Media: Does the practice dispose of devices and media in a fashion that prevents the disclosure of PHI?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Removal of Devices and Media: When the practice removes devices and media from the practice site, e.g., a portable computer or a PDA, does the practice treat the device or media in the same fashion that it treats paper medical records?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

Technical Safeguards

Personal or "Entity" Authentication

Identification and Authentication
--

	Does the practice issue each member of the workforce a unique user name and an initial password?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Are passwords changed at least once every 90 days?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Does the practice use the standard password protection programs for log on and in each of the programs in which it stores PHI?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Are workforce members educated regarding the appropriate choice of passwords (e.g., no names) and the need to keep passwords confidential?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Are workforce members educated to not keep passwords in written or electronic form in the practice and to not share passwords?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Automatic Logoff			
	Does the practice require that all computers “lock up” and require an individual to sign on after a 15-minute period of not being used?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Does the practice configure its computers such that another individual is not able to access the computer until the first individual re-enters his or her password and then logs off the system?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Password Deletion: Does the Security Officer delete passwords when a workforce member is terminated or no longer has rights to access a particular system or computer?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Documentation, Testing, Inventory, Virus Control			
	Testing: Does the practice periodically test all hardware and software to ensure that it meets the practice’s security policies and procedures?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Inventory: Does the practice have an inventory of all hardware and software used by the practice?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Virus Detection: Does the practice have in place a virus detection program to protect the practice’s data, run a virus scan on each of its computers daily, and update the virus protection on a regular basis?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Firewall: Does the practice have in place an up-to-date firewall program to protect the practice’s data?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Windows Update: Does the practice use the Windows operating system and check at least once a week for critical updates by running the “Windows Update”?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	NOTE: If the practice <i>does not use the Windows operating system</i> , then the previous paragraph needs to be changed to reflect how the practice’s operating system is updated in accordance with the system vendor’s recommendations.		
Transmission Security			
	NOTE: The model policies and procedures included above assume that you are not sending or receiving PHI electronically, e.g., via e-mail or over the Internet. If you do send any PHI electronically, the practice must ensure the “transmission security” of the PHI.	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Does the practice use a program to protect PHI sent electronically, e.g., locking all data files?		

Other Administrative Policies and Procedures

Security Officer			
	Does the practice have a Security Officer?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

Does the practice document who is the Security Officer and maintain that document for six years?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
--	------------------------------	-----------------------------

Information Access Management

Does the practice allow all members of its workforce to have access to all PHI as necessary for them to carry out their job functions and support the efficient operation of the practice?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Does the practice limit access to PHI to that information necessary for a member of its workforce to carry out his or her job functions?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Does the Security Officer monitor the practice's operations to ensure that all workforce members are accessing PHI appropriately?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

Security Incident Procedures

Does the practice monitor information system activity to detect security incidents?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Does the practice record and follow up when it determines someone or some program has entered its computer system from outside the practice or someone inside the practice accesses, uses, or changes PHI in an unauthorized manner?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
If there have been harmful effects, does the Security Officer take steps to mitigate those harmful effects?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Does the practice train the workforce to deal with security incidents and minimize harmful effects of security incidents?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

Awareness and Training for Staff

Does the practice provide training to its workforce with respect to the security of protected health information (PHI), have ongoing training and periodic training updates, and document that each member of the workforce is trained?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
---	------------------------------	-----------------------------

Workforce Sanctions

Does the practice apply appropriate sanctions against workforce members who fail to comply with the practice's security policies and procedures?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Is the particular sanction dependent on the harm created by the unauthorized use or disclosure of PHI, whether the use or disclosure was intentional or unintentional, and whether or not the workforce member has previously used or disclosed PHI in violation of the practice's policies and procedures?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Does the practice have in place exceptions to applying the sanctions to workforce members in the case of a "whistleblower," crime victim, and complaints and investigations?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Does the practice document all sanctions taken against workforce members in its personnel files and maintain this information for a period of six years from the date of its creation?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

Risk Analysis, Risk Management, and Ongoing Risk Evaluation

Risk Analysis: Has the practice completed this risk analysis?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Risk Management: Has the practice addressed any item for which you answered "No" on this risk analysis? <i>If not, now is the time to do such to ensure your practice meets the requirements of the Security Rule.</i>	<input type="checkbox"/> Yes	<input type="checkbox"/> No

Ongoing Evaluation: Is the practice planning to update this risk analysis on an ongoing basis?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
---	------------------------------	-----------------------------

Appendices

Model Notice of Privacy Practices

NOTE: THIS MODEL NOTICE IS BASED ON THE MODEL POLICIES AND PROCEDURES INCLUDED IN THIS DOCUMENT. YOU WILL NEED TO MODIFY THIS MODEL NOTICE TO THE EXTENT YOU NEED TO MODIFY THE POLICIES AND PROCEDURES FOR YOUR PRACTICE.

IN ADDITION, THE NOTICE CAN USE A SMALLER FONT, BUT IT IS RECOMMENDED THAT THE NOTICE BE IN AT LEAST 10 POINT TYPE.

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

This practice creates a medical record of your health information in order to treat you, receive payment for services delivered, and to comply with certain policies and laws. We are also required by law to provide you with this Notice of our legal duties and privacy practices. In addition, the law requires us to ask you to sign an Acknowledgment that you received this Notice.

We are required by federal and state law to maintain the privacy of your medical information. Medical information is also called “protected health information” or “PHI.”

This is a list of some of the types of uses and disclosures of PHI that may occur:

Treatment: We obtain health information, or PHI, about you to treat you. Your PHI is used by us and others to treat you. We may also send your PHI to another physician, facility, or counselor to which we refer you for treatment, care, procedures, or testing. We may also use your PHI to contact you to tell you about alternative treatments or other health-related benefits we offer. If you have a friend or family member involved in your care, we may give them PHI about you.

Payment: We use your PHI to obtain payment for the services that we render. For example, we send PHI to Medicaid, Medicare, or your insurance plan to obtain payment for our services.

Health Care Operations: We use your PHI for our operations. For example, we may use your PHI in determining whether we are giving adequate treatment to our patients. From time-to-time, we may use your PHI to contact you to remind you of an appointment.

Legal Requirements: We may use and disclose your PHI as required or authorized by law. For example, we may use or disclose your PHI for the following reasons:

Public Health: We may disclose your health information to prevent or control disease, injury, or disability; to report births and deaths, to report reactions to medicines or medical devices, or to report suspected cases of abuse or neglect.

Health Oversight Activities: We may use and disclose your PHI to state agencies and federal government authorities when required to do so. We may use and disclose your health information in order to assist others in determining your eligibility for public benefit programs and to coordinate delivery of those programs. For example, we must give PHI to the Secretary of Health and Human Services in an investigation into our compliance with the federal privacy rule.

Judicial and Administrative Proceedings: We may use and disclose your PHI in judicial and administrative proceedings. Efforts may be made to contact you prior to a disclosure of your PHI to the party seeking the information.

Law Enforcement: We may use and disclose your PHI in order to comply with requests pursuant to a court order, warrant, subpoena, summons, or similar process. We may use and disclose PHI to locate someone who is missing, to identify a crime victim, to report a death, to report criminal activity at our offices, or in an emergency.

Avert a Serious Threat to Health or Safety: We may use or disclose your PHI to stop you or someone else from getting hurt.

Work-Related Injuries: We may use or disclose PHI to an employer if the employer is conducting medical workplace surveillance or to evaluate work-related injuries.

Coroners, Medical Examiners, and Funeral Directors: We may use or disclose PHI to a coroner or medical examiner in some situations. For example, PHI may be needed to identify a deceased person or determine a cause of death. Funeral directors may need PHI to carry out their duties.

Armed Forces: We may use or disclose the PHI of Armed Forces personnel to the military for proper execution of a military mission. We may also use and disclose PHI to the Department of Veterans Affairs to determine eligibility for benefits.

National Security and Intelligence: We may use or disclose PHI to maintain the safety of the President or other protected officials. We may use or disclose PHI for the conduct of national intelligence activities.

Correctional Institutions and Custodial Situations: We may use or disclose PHI to correctional institutions or law enforcement custodians for the safety of individuals at the correctional institution, those that are responsible for transporting inmates, and others.

Research: You will need to sign an Authorization form before we use or disclose PHI for research purposes except in limited situations. For example, if you want to participate in research or a clinical study, an Authorization form must be signed.

Fundraising: If we undertake any fundraising activities, we may contact you about the fundraising activity. We do not engage in marketing activities and need your authorization to do so.

Your Rights: You have certain rights under federal and state laws relating to your PHI. Some of these rights are described below:

Restrictions: You have a right to request restrictions on how your PHI is used for purposes of treatment, payment, and health care operations. We are not required to accommodate your request.

Communications: You have a right to receive confidential communications about your PHI. For example, you may request that we only call you at home. If your request is reasonable, it may be accepted.

Inspect and Access: You have a right to inspect your health information. This information includes billing and medical record information. You may not inspect your record in some cases. If your request to inspect your record is denied, we will send you a letter letting you know why and explaining your options.

You may have a copy of your PHI in most situations. If you request a copy of your PHI, we may charge you a fee for making the copies and mailing them to you, if you ask us to mail them.

Amendments of Your Records: If you believe there is an error in your PHI, you have a right to request that we amend your PHI. We are not required to agree with your request to amend.

Accounting of Disclosures: You have a right to receive an accounting of disclosures that we have made of your PHI for purposes other than treatment, payment, and health care operations, or release made pursuant to your authorization.

Copy of Notice: You have a right to obtain a paper copy of this Notice, even if you originally received the Notice electronically. We have also posted this Notice at our offices.

Complaints: If you feel that your privacy rights have been violated, you may file a complaint with us by calling our Privacy Officer at (____)____-____. We will not retaliate against you for filing a complaint. You may also file a complaint with the Secretary of Health and Human Services in Washington, DC, if you feel your privacy rights have been violated.

We are required to abide with terms of the Notice currently in effect; however, we may change this Notice. If we materially change this Notice, you can get a revised Notice [*on our website at www._____.____, or*] by stopping by our office to pick up a copy. Changes to the Notice are applicable to the health information we already have.

EFFECTIVE DATE: _____

Model Business Associate Agreement

This Agreement is made this _____ day of _____, 2004, by [*Physician name and address*] (Practice), and [*Business Associate name and address*] (Business Associate). The parties are desirous of entering into this Agreement in order to comply with federal law.

I. DEFINITIONS

A. Business Associate. “Business Associate” shall mean [*Business Associate name and address*].

B. Covered Entity. “Covered Entity” shall mean Practice.

C. “Electronic Protected Health Information” shall have the meaning found in the Security Rule. [45 CFR § 160.103.]

D. Individual. “Individual” means a person and includes a personal representative who under law has authority to make health decisions for another person. [45 CFR § 164.502(g)].

E. Privacy Rule. “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.

F. Protected Health Information. “Protected Health Information” means individually identifiable health information that is transmitted or maintained in any form or medium, limited to the information created or received by Business Associate from or on behalf of Covered Entity. [45 CFR § 160.103]

G. Required By Law. “Required By Law” means a mandate contained in law that compels use or disclosure of protected health information and that is enforceable in a court of law including but not limited to subpoenas. [45 CFR § 164.103].

H. Security Rule. “Security Rule” shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Part 160 and Part 164, Subparts A and C.

I. Secretary. “Secretary” means the Secretary of the Department of Health and Human Services or his designee.

II. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

A. Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by the Agreement or as Required By Law, such as mandated reports to regulatory agencies.

B. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement.

C. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

D. Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.

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

F. ***[This section is not necessary if business associate does not have protected health information in a designated record set.]*** Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner ***[access policy such as - upon 10 business days written notice during regular business hours of 10am - 4pm, unless an alternative time is agreed upon by the Covered Entity and the Business Associate]***, to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual. [45 CFR § 164.524.] Business associate designated record set means ***[specify]***.

G. ***[This section is not necessary if business associate does not have protected health information in a designated record set.]*** Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to the request of Covered Entity or an Individual, and in the time and manner ***[access policy such as - upon 10 business days written notice during regular business hours of 10am - 4pm, unless an alternative time is agreed upon by the Covered Entity and the Business Associate]***. Business associate designated record set means ***[specify]***.

H. Business Associate agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Covered Entity, or to the Secretary, in a time and manner ***[access policy such as upon 10 business days written notice during regular business hours of 10am - 4pm, unless an alternative time is agreed upon by the Covered Entity and the Business Associate]*** or designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule and Security Rule.

I. Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information [45 CFR § 164.528]. Business Associate agrees to provide to Covered Entity or an Individual, in time and manner ***[access policy such as - upon 10 business days written notice during regular***

business hours of 10am - 4pm, unless an alternative time is agreed upon by the Covered Entity and the Business Associate], information collected in accordance with this Section of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information. [45 CFR § 164.528].

J. Business Associate shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic Protected Health Information that it creates, receives, maintains, or transmits on behalf of the Covered Entity as required by the Security Rule.

K. Business Associate shall ensure that any agent, including a subcontractor, to whom it provides electronic Protected Health Information agrees to implement reasonable and appropriate safeguards to protect it.

L. Business Associate shall report to Covered Entity any security incident of which it becomes aware.

M. Business Associate agrees NOT to seek an Authorization to allow marketing to individuals whose protected health information is created or received in carrying out the duties under this Agreement.

III. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE – GENERAL USE AND DISCLOSURE PROVISIONS

[(A) AND (B) are alternative approaches]

A. Specify purposes: Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, Covered Entity for the following purposes, if such use or disclosure of Protected Health Information would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity:

[Explicitly state business associate purpose for having PHI in general terms].

B. Refer to underlying services agreement: Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in *[refer to underlying service contract]*, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

IV. SPECIFIC USE AND DISCLOSURE PROVISIONS

A. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

B. Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are Required By Law or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

C. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity. [45 CFR § 164.504(e)(2)(i)(B)].

D. Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities [45 CFR § 164.502(j)(1)].

V. OBLIGATIONS OF COVERED ENTITY – PROVISIONS FOR COVERED ENTITY TO INFORM BUSINESS ASSOCIATE OF PRIVACY PRACTICES AND RESTRICTIONS

Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information. [45 CFR § 164.522].

VI. PERMISSIBLE REQUESTS BY COVERED ENTITY

Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity except when the Business Associate uses or discloses Protected Health Information for data aggregation or management and administrative activities of Business Associate.

VII. TERM AND TERMINATION

A. Term. The Term of this Agreement shall be effective as of the date specified above and shall terminate: for cause, as outlined below; or when all of the Protected Health Information provided by Covered Entity to Business Associate or created or received by Business Associate on behalf of Covered Entity is destroyed or returned to covered entity. If it is not feasible to return or destroy Protected Health Information, Business Associate shall extend protections to such information in accordance with the termination provisions in this Section.

B. Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall:

1. Provide written notice to and 45 days for Business Associate to cure the breach or end the violation and terminate this Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;

2. Immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible; or

3. If neither termination nor cure are feasible, Covered Entity shall report the violation to the Secretary.

C. Effect of Termination.

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

2. In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make destruction infeasible. Upon written confirmation that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the destruction infeasible, for so long as Business Associate maintains such Protected Health Information, except as required by law.

VIII. MISCELLANEOUS

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

B. Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191. In the event Covered Entity believes in good faith that any provision of this Agreement fails to comply with the then-current requirements of the Health Insurance Portability and Accountability Act and the rules promulgated thereunder, the Covered Entity shall notify Business Associate in writing. For a period up to thirty (30) days, the parties shall address such concern in good faith and seek to amend the terms of this Agreement to bring it into compliance. If after such thirty-day period this Agreement fails to come into compliance, then the Agreement may be terminated by the Covered Entity in accordance with the notice provisions of the Underlying Agreement.

C. Survival. The respective rights and obligations of Business Associate under Section VII (C) of this Agreement shall survive the termination of this Agreement.

D. Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.

E. Choice of Law. This Agreement will be governed by the laws of the State of South Dakota.

F. Severability. In the event that any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, the remainder of the provisions of this Agreement will remain in full force and effect.

Practice

Business Associate

Type Name & Address

Type Name & Address

Date _____