

HIPAA POLICY HANDBOOK

Privacy and Security Policies, Procedures and Documentation

This document provided by WorkSmart MD and extracted from the HIPAA Rx™ Compliance Software

The HIPAA standards for privacy and security require the development and adoption of policies and procedures to facilitate compliance with the HIPAA requirements. The sample policy handbook that is included with HIPAA Rx contains model policies and procedures that address the primary HIPAA privacy and security requirements for healthcare providers. It is important to carefully read and review the policies and procedures as you customize them. The documents are very comprehensive and depending on the size of your organization may need to be adjusted to reasonably and appropriately address the needs of your specific business environment.

Customizing these documents alone will not make your organization HIPAA compliant. It is critical that if your organization adopts the policies and procedures contained in this manual it adheres to them. As written in section 164.316(b)(2)(i) of the security standards all documentation must be maintained for six-years from the date of creation or the date when it was last in effect, whichever is later.

As you read the policies and procedures you will notice that certain text is [red] and is enclosed in brackets. In these instances you will need to customize the text. If you would like to quickly insert the name of your organization it is recommended that you do a “Find and Replace.” In Microsoft Word you can do this by selecting “Edit” and then selecting “Replace.” You will want to find [NAME OF ORGANIZATION] and replace it with the name of your business.

Table of Contents
HIPAA Policies and Procedures

DESCRIPTION OF POLICIES AND PROCEDURES.....3
POLICY FOR GENERAL USES AND DISCLOSURES OF PHI.....9
POLICY FOR PATIENT RIGHTS TO HEALTH INFORMATION..... 11
POLICY FOR IDENTITY VERIFICATION OF INDIVIDUALS REQUESTING PHI 13
POLICY FOR DISCLOSURES OF PHI TO FAMILY AND FRIENDS..... 16
POLICY FOR ACCESSING AND INSPECTING PHI..... 18
POLICY FOR ACCOUNTING OF DISCLOSURES 22
POLICY FOR HEALTH RECORD AMENDMENT..... 24
POLICY FOR ACCEPTING AND DENYING RESTRICTIONS OF PHI..... 26
POLICY FOR MINIMUM NECESSARY USES AND DISCLOSURES OF PHI 28
POLICY FOR USE AND DISCLOSURE OF PSYCHOTHERAPY NOTES..... 30
POLICY FOR USE AND DISCLOSURE OF PHI FOR MARKETING..... 32
POLICY FOR USE AND DISCLOSURE OF PHI FOR JUDICIAL PROCEEDINGS 34
POLICY FOR USE AND DISCLOSURE OF PHI TO DHHS..... 37
POLICY FOR EDUCATING AND TRAINING MEMBERS OF THE WORKFORCE..... 39
POLICY FOR DISCLOSURES TO BUSINESS ASSOCIATES 41
POLICY FOR MITIGATION AFTER IMPROPER USE OR DISCLOSURE OF PHI..... 44
POLICY FOR NON-RETALIATION AGAINST EMPLOYEES 46
POLICY FOR SECURING ELECTRONIC HEALTH INFORMATION..... 48
POLICY FOR ACCESS TO PHI BY WORKFORCE MEMBERS..... 51
POLICY FOR ACCEPTABLE WORKSTATION USE 53
POLICY FOR ELECTRONIC DATA ACCESS..... 55
POLICY FOR DATA CLASSIFICATION..... 57
POLICY FOR PASSWORD PROTECTION..... 60
POLICY FOR INSTANT MESSAGING..... 62
POLICY FOR A CCEPTABLE USE OF EMAIL 64
POLICY FOR TRANSMITTING AND RECEIVING ELECTRONIC PHI..... 67
POLICY FOR FAX TRANSMITTAL OF PHI..... 69
POLICY FOR MEDIA CONTAINING ELECTRONIC PHI..... 72
POLICY FOR MAINTAINING PHYSICAL SECURITY 74
POLICY FOR THE RETENTION OF DOCUMENTATION..... 76
POLICY FOR THE DISPOSAL OF PHI..... 78
POLICY FOR REPORTING SECURITY INCIDENTS..... 81
POLICY FOR PREVENTING AND DETECTING SECURITY VIOLATIONS..... 83
POLICY FOR VIOLATIONS OF INTERNAL PROCEDURES 85
POLICY FOR SANCTIONING AND DISCIPLINING EMPLOYEES..... 89
POLICY FOR TERMINATION OF EMPLOYEES 93
WORKFORCE STATEMENT OF UNDERSTANDING..... 96

DESCRIPTION OF POLICIES AND PROCEDURES

The following documentation should be customized during your HIPAA project; all documentation should be placed in your compliance manual and/or employee handbook. A description of each document is provided

HIPAA PRIVACY POLICIES AND PROCEDURES

Policy for General Uses and Disclosures of PHI

The purpose of this policy is to establish guidelines and protocols that must be followed by management and workforce members regarding the uses and disclosures of protected health information (PHI).

Policy for Patient Rights to Health Information

The purpose of this policy is to provide information for management and workforce members about the privacy rights that patients have regarding their health information.

Policy for Identity Verification of Individuals Requesting PHI

The purpose of this policy is to provide guidance for management and workforce members regarding the verification of identity and authority of requestors of protected health information.

Policy for Disclosures of PHI to Family and Friends

The purpose of this policy is to provide information for management and workforce members regarding the disclosures of a patient's protected health information (PHI) to a patient's family and friends.

Policy for Accessing and Inspecting PHI

The purpose of this policy is to provide instructions for management and workforce members regarding access to protected health information by patients, parents, guardians and personal representatives.

Policy for Accounting of Disclosures

The purpose of this policy is to provide management and workforce members with a standard procedure for accounting of all disclosures of patients protected health information.

Policy for Health Record Amendment

The purpose of this policy is to provide management and workforce members with a standard procedure to patients requesting an amendment to their protected health information.

Policy for Accepting and Denying Restrictions of PHI

The purpose of this policy is to provide management and members of the workforce with a standard procedure for restricting access to patient's protected health information.

Policy for Minimum Necessary Uses and Disclosures of PHI

The purpose of this policy is to provide management and workforce members with a standard procedure for keeping health information on a need-to-know basis and maintaining the confidentiality patient's medical history.

Policy for Use and Disclosure of Psychotherapy Notes

The purpose of this policy is to provide information for management and workforce members regarding the use and disclosure of a patient's psychotherapy notes.

Policy for Use and Disclosure of PHI for Marketing

The purpose of this policy is to establish guidelines for management and workforce members regarding the use and disclosure of a patient's protected health information (PHI) for marketing.

Policy for Use and Disclosure of PHI for Judicial or Administrative Proceedings

The purpose of this policy is to provide guidance for management and workforce members regarding the use and disclosure of a patient's protected health information (PHI) judicial and administrative proceedings.

Policy for Use and Disclosure of PHI to the Department of Health and Human Services

The purpose of this policy is establish guidelines for management and workforce members regarding the use and disclosure of a patient's protected health information (PHI) to the Department of Health and Human Services (DHHS).

Policy for Educating and Training Members of the Workforce

The purpose of this policy is to provide guidance for management and workforce members regarding mandatory workforce training as required by the Health Insurance Portability and Accountability Act (HIPAA).

Policy for Disclosures to Business Associates

The purpose of this policy is to provide management and workforce members with procedures and protocols that must be followed by management and workforce members regarding disclosures to business associates.

Policy for Mitigation after Improper Use or Disclosure of PHI

The purpose of this policy is to provide procedure to management and workforce members for mitigating the harmful effects of a use or disclosure of protected health information that violates the policies and procedures of the organization.

Policy for Non-Retaliation against Employees

The purpose of this policy is to provide procedures for management and workforce members regarding non-retaliation in cases involving the reporting of violations or infractions of HIPAA or other federal or state laws or regulatory requirements.

HIPAA SECURITY POLICIES AND PROCEDURES

Policy for Securing Electronic Health Information

The purpose of this policy is to provide guidance for management and workforce members in establishing practices which secure protected health information in electronic forms.

Policy for Access to PHI by Members of the Workforce

The purpose of this policy is to provide guidance for management and workforce members regarding access to protected health information and to ensure that they recognize the importance of maintaining the confidentiality, security and integrity of protected health information.

Policy for Acceptable Workstation Use

The purpose of this policy is to establish guidelines for management and workforce members on the proper functions and physical attributes of the surroundings of workstations that access protected health information.

Policy for Electronic Data Access

The purpose of this policy is to establish guidelines for management and workforce members regarding the access of electronic protected health information.

Policy for Data Classification

The purpose of this data access policy is to provide a system for protecting information that is critical to the organization. All employees that interact with confidential information are expected to familiarize themselves with this and follow its guidelines.

Policy for Password Protection

This policy outlines the handling, responsibilities, and scope of passwords for the information systems of the organization.

Policy for Instant Messaging

The purpose of this policy is to establish guidelines for management and workforce members for the appropriate use of instant messaging within the organization.

Policy for Acceptable Use of E-mail

The purpose of this policy is to define appropriate standards for management and workforce members for secure and effective use of the electronic mail system within the organization.

Policy for Transmitting & Receiving Electronic PHI

The purpose of this policy is to establish guidelines for management and workforce members regarding the security of electronic transmissions.

Policy for Fax Transmittal of PHI

The purpose of this policy is to establish guidelines for management and workforce members regarding the transmission and receipt of protected health information by facsimile (fax).

Policy for Media Containing Electronic PHI

The purpose of this policy is to establish guidelines for management and workforce members regarding the receipt, removal and storage of hardware and electronic media that contain electronic protected health information.

Policy for Maintaining Physical Security

The purpose of this policy is to establish guidelines for management and workforce members regarding the limit of physical access to electronic information systems and the facility in which they are housed.

Policy for the Retention of Documentation

The purpose of this policy is to establish guidelines for management and workforce members regarding the retention and maintenance of documentation created during the HIPAA compliance process.

Policy for the Disposal of PHI

The purpose of this policy is to provide management and workforce members with the procedures for the proper disposal of protected health information.

Policy for Reporting Security Incidents

The purpose of this policy is to establish guidelines for management and workforce members for identifying and responding to suspected or known security incidents.

Policy for Preventing and Detecting Security Violations

The purpose of this policy is to establish guidelines for management and workforce members regarding the prevention, detection, and correction of security violations.

Policy for Violations of Internal Policies

The purpose of this policy is to provide information for management and workforce specifying enforcement, penalty, and disciplinary actions that may result from violation of policies regarding the privacy and protection of an individual's protected health information (PHI) and to offer guidelines on how to conform to the required standards.

Policy for Sanctioning and Disciplining Employees

The purpose of this policy is to provide guidance for management and workforce members regarding the disciplinary and dismissal policies and procedures to workforce members when breaches of the HIPAA Regulations or the organization's policies occur.

Policy for Termination of Employees

The purpose of this policy is to provide guidance for management and workforce members regarding the termination of employees that have violated the policies and procedures of the organization.

POLICY FOR GENERAL USES AND DISCLOSURES OF PHI

[Insert Logo or Organization Name]

Corporate Privacy Policy

Dates: **Latest Revision:** April 14, 2003

Replaces: **Original Effective Date:**

Purpose

The purpose of this policy is to establish guidelines and protocols that must be followed by management and workforce members regarding the uses and disclosures of protected health information (PHI).

Policy

All individuals obtaining treatment from [NAME OF ORGANIZATION] should receive a Notice of Privacy Practices that explains the individual's rights and [NAME OF ORGANIZATION]'s legal duties regarding protected health information. This notice provides the individual with a clear definition of the uses and disclosures that will be made by [NAME OF ORGANIZATION].

[Name of Health Care Provider or Practice]'s workforce members may use and disclose protected health information for Treatment, Payment and Health Care Operations (TPO) without written authorization from patients.

It is permissible to disclose PHI to business associates where [NAME OF ORGANIZATION] has obtained signed business associate contracts that require the business associate to safeguard the protected health information.

It is permissible to disclose PHI to another physician or healthcare provider that is providing treatment a patient.

For uses and disclosures that are not for treatment, payment, or healthcare operations a signed Authorization to Use and Disclose PHI must be on file.

Definitions

See glossary for key terms and acronyms used in this policy.

Enforcement

Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

Rationale/ Source

This policy complies with requirements of the following:

- Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations

**Cross
References**

For additional information, refer to the following:

Document Name
Notice of Privacy Practices Policy for Access to PHI by Workforce Members

**Review or
Revision Date**

This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance

Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Privacy Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR PATIENT RIGHTS TO HEALTH INFORMATION

[Insert Logo or Organization Name]

Corporate Privacy Policy

Dates: **Latest Revision:** April 14, 2003

Replaces: **Original Effective Date:**

Purpose

The purpose of this policy is to provide information for management and workforce members about the privacy rights that patients have regarding their health information.

Policy

As written in the HIPAA privacy rule patients are provided with the following rights regarding their health information:

Patients may access and copy their health information, consistent with certain limitations;

Patients may receive an accounting of disclosures **[NAME OF ORGANIZATION]** has made of their protected health information (PHI) for up to six years prior to the date of requesting such accounting. Information may not be available prior to the effective date of this policy (April 14, 2003) and certain limitations do apply as outlined in the Policy for Accounting of Disclosures;

Patients may submit complaints if they believe or suspect that information about them has been improperly used or disclosed;

If a patient believes that health information in their record is inaccurate the patient may request **[NAME OF ORGANIZATION]** to amend the health information;

Patients may ask **[NAME OF ORGANIZATION]** to take specific actions regarding the use and disclosure of their information and **[NAME OF ORGANIZATION]** may either approve or deny the request. Specifically, patients have the right to request:

1. That **[NAME OF ORGANIZATION]** restrict uses and disclosures of their individual information while carrying out treatment, payment activities, or health care operations.
2. To receive information from **[NAME OF ORGANIZATION]** by alternative means, such as mail, e-mail, fax or telephone, or at alternative locations.

Patients may request to receive confidential communications about their health information.

Each patient of **[NAME OF ORGANIZATION]** will receive a "*Notice of Privacy Practices*" that clearly explains the individual's rights regarding his/her health information.

Definitions See glossary for key terms and acronyms used in this policy.

Enforcement Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

Rationale/Source This policy complies with requirements of the following:

- Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations

Cross References For additional information, refer to the following:

Document Name
Notice of Privacy Practices
Policy for Accounting of Disclosures
Policy for Health Record Amendment
Policy for Access to PHI
Policy for the Inspection of PHI

Review or Revision Date This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Privacy Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR IDENTITY VERIFICATION OF INDIVIDUALS REQUESTING PHI

[Insert Logo or Organization Name]

Corporate Privacy Policy

Dates: **Latest Revision: April 14, 2003**
Original Effective Date:
Replaces:

Purpose

The purpose of this policy is to provide guidance for management and workforce members regarding the verification of identity and authority of requestors of protected health information.

Policy

[NAME OF ORGANIZATION]'s Privacy Officer, and other staff and workforce members, shall verify the identity of requestors of protected health information and ensure the requestor has the proper authority to request such information.

Procedure

A valid authorization for the disclosure of protected health information must be obtained before the health information can be obtained to any third party requesting the information. The requestor must present identification prior to receipt of any records regarding themselves.

[NAME OF ORGANIZATION]'s Privacy Officer or designee staff may rely on the following information to demonstrate identity:

1. Presentation of agency identification, credentials or other proof of government status (a badge, identification card, etc.);
2. A written request on agency letterhead or an oral statement if a written statement would not be possible (a natural disaster, other emergency situations, etc.);
3. If the disclosure is requested by a person acting on behalf of a public official, a written statement on government letterhead that the person is acting under the government's authority, or a contract or purchase order evidencing the same; or
4. A court order.

[NAME OF ORGANIZATION]'s Privacy Officer or designee shall verify identity of any phone requests from all individuals, including law enforcement officers and others who have an official need for PHI by using a callback phone number before releasing information.

Procedure

[NAME OF ORGANIZATION]'s Privacy Officer or designee shall verify facsimile number of any faxed requests. The main number of the sending agency shall be called, and the fax number verified. Fax machines shall be set to imprint the origin. All incoming faxes shall be reviewed for imprint origin.

[NAME OF ORGANIZATION]'s Privacy Officer or designee shall verify e-mail address by calling requestor. The general number for the sending agency shall be called, and then a request shall be made to be transferred to the specific individual who made the contact.

[NAME OF ORGANIZATION]'s Privacy Officer or designee personnel are responsible for copying verification information or obtaining badge number, etc., and for creating a file for the requestor and for maintaining the information in the requestor's file.

[NAME OF ORGANIZATION]'s Privacy Officer or designee may disclose information to the requestor if all requirements for use and disclosure are met, and if all requirements within this policy are met. If identify is not verified Privacy Officer or designee may deny access to health information.

[NAME OF ORGANIZATION]'s Privacy Officer shall assure that a mechanism is in place which tracks disclosure of both written and verbal protected health information. The same format shall be utilized for all facilities.

Definitions

See glossary for key terms and acronyms used in this policy.

Enforcement

Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

**Rationale/
Source**

This policy complies with requirements of the following:

- Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations Section 164.514(h)(1)

**Cross
References**

Document Name
For additional information, refer to the following: Policy for Minimum Necessary Policy for General Uses and Disclosures of PHI

**Review or
Revision Date**

This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance

Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Privacy Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR DISCLOSURES OF PHI TO FAMILY AND FRIENDS

[Insert Logo or Organization Name]

Corporate Privacy Policy

Dates: **Latest Revision: April 14, 2003**

Replaces: **Original Effective Date:**

Purpose

The purpose of this policy is to provide information for management and workforce members regarding the disclosures of a patient's protected health information (PHI) to a patient's family and friends.

Policy

[NAME OF ORGANIZATION] may disclose to a family member, other relative, a close personal friend of the individual, or any other person identified by the individual, the PHI directly relevant to such person's involvement with the individual's care or payment related to the individual's health care.

[NAME OF ORGANIZATION] may use or disclose PHI to notify or to assist in the notification of a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death.

[NAME OF ORGANIZATION] can also use and disclose PHI in these circumstances for identifying or locating the individual's family members, personal representative, or other persons responsible for the care of the individual.

In order for **[NAME OF ORGANIZATION]** to use or disclose PHI for these purposes, the individual's presence is a determining factor. The following processes outline how **[NAME OF ORGANIZATION]** may use and disclose PHI for these purposes.

Uses and Disclosures with the Individual Present

If the individual is present for or otherwise available prior to, a use or disclosure and has the capacity to make health care decisions, **[NAME OF ORGANIZATION]** may use or disclose the PHI if it:

1. Obtains the individual's agreement;
2. Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or
3. Reasonably infers from the circumstances, based on the exercise of professional judgment that the individual does not object to such disclosure.

Policy

Limited Uses and Disclosures When the Individual is Not Present

If the individual is not present or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual’s incapacity or an emergency circumstance, **[NAME OF ORGANIZATION]** may, in exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the PHI that is directly relevant to the person’s involvement with the individual’s health care.

[NAME OF ORGANIZATION] may use professional judgment and its experience with common practice to make reasonable inferences of the individual’s best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X rays, or other similar forms of PHI.

Definitions

See glossary for key terms and acronyms used in this policy.

Enforcement

Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

**Rationale/
Source**

This policy complies with requirements of the following:
• Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations Section 164.510(b)

**Cross
References**

For additional information, refer to the following:

Document Name

**Review or
Revision Date**

This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance

Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Privacy Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR ACCESSING AND INSPECTING PHI

[Insert Logo or Organization Name]

Corporate Privacy Policy

Dates: **Latest Revision:** April 14, 2003

Replaces: **Original Effective Date:**

Purpose

The purpose of this policy is to provide instructions for management and workforce members regarding access to protected health information by patients, parents, guardians and personal representatives.

Policy

It is the policy of [NAME OF ORGANIZATION] to protect the privacy of individually identifiable health information. In cases where the patient has been civilly adjudicated, or is incapacitated or is a minor, the parent or the legal guardian or personal representative may request access. An exception can occur when a minor signs in for substance abuse treatment without parental consent, and in that situation, parents shall not have access to the protected health information. There may be additional exceptions as allowed by law.

Procedure

A patient who has or is receiving services from [NAME OF ORGANIZATION], or a parent of a minor, or a personal representative or a legal guardian must request in writing for access to inspect, or receive copies of protected health information.

The "Request for Inspection of PHI" form shall be provided to facilitate the request. [NAME OF ORGANIZATION] personnel may assist in initiating the process requesting inspection of protected health information.

All requests by patients and their legal representatives for PHI must be forwarded to [NAME OF ORGANIZATION]'s Privacy Officer for action.

If it is acceptable after discussion with the patient, [NAME OF ORGANIZATION] may provide a summary of the PHI to the patient. If the summary is acceptable, [NAME OF ORGANIZATION] shall determine the appropriate staff to provide that explanation to the patient. The patient's agreement to a summary and agreement to any costs associated with the summary shall be documented in writing.

This request shall be processed in the format requested i.e. microfiche, computer disk, etc, if possible, and in a timely consistent manner according to established timeframes but not more than 30 days after receipt of the request. If the record cannot be accessed within the 30 days, the timeframe may be extended once for no more than an additional 30 days with notification in writing to the individual outlining reasons for the delay and the date the request will be concluded.

A **“Request for Inspection of PHI”** may be denied without a right to review as follows:

1. If the information conforms to one of the following categories: psychotherapy notes; information compiled for use in a civil, criminal or administrative action or proceeding; or information that would be prohibited from use or disclosure under the Certified Laboratory Information Act (CLIA) laws and regulations;
2. If the patient is participating in research related treatment and has agreed to the denial of access to records for the duration of the study;
3. If access is otherwise precluded by law;
4. 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; or
5. If **[NAME OF ORGANIZATION]** has been provided a copy of a court order from a court of competent jurisdiction which limits the release or use of PHI.

A **“Request for Inspection of PHI”** may be denied provided the individual is given a right to have the denial reviewed as follows:

1. A licensed health care professional based on an assessment of the particular circumstances, determines that the access requested is reasonably likely to endanger the life or physical safety of the patient or another person.
2. **[NAME OF ORGANIZATION]** may deny the patient access to PHI if the information requested makes reference to someone other than the patient and a licensed health care professional has determined that the access requested is reasonably likely to cause serious harm to that other person.
3. **[NAME OF ORGANIZATION]** may deny a request to receive a copy or inspect PHI by a personal representative of the patient if **[NAME OF ORGANIZATION]** has a reasonable belief that the patient has been or may be subjected to domestic violence, abuse, or neglect by such person; or treating such person as the personal representative could endanger the individual; and **[NAME OF ORGANIZATION]**, exercising professional judgment, decides that it is not in the best interest of the patient to treat that person as the patient’s personal representative.

Denial of Access

Upon denial of any request for access to PHI, in whole or in part, a written letter shall be sent to the patient, or other valid representative making the request for access, stating in plain language the basis for the denial.

If the patient has a right to a review of the denial as outlined above, the letter shall contain a statement of how to make an appeal of the denial including the name, title, address, and telephone number of the person to whom an appeal should be addressed.

This letter shall also address the steps to file a complaint with the secretary of HHS.

If the information requested is not maintained by **[NAME OF ORGANIZATION]**, but it is known where the patient may obtain access, **[NAME OF ORGANIZATION]** must inform the patient where to direct the request for access.

Appeal and Denial of Requests

A patient, parent of a minor, or guardian of a patient has the right to appeal the decision to withhold portions or all of the record for safety or confidentiality reasons.

The appeal shall be submitted in writing to **[NAME OF ORGANIZATION]**'s Privacy Officer who will then designate a licensed health care professional who did not participate in the original decision.

The designated licensed health care professional who did not participate in the original decision to deny access shall review the record and the request for access to the patient's record.

1. The reviewer must determine if access meets an exception as described above.
2. If the reviewer determines that the initial denial was appropriate, the patient must be notified in writing, using plain language, that the review resulted in another denial of access. The notice must include the reasons for denial and must describe the process to make a complaint to the Secretary of HHS.
3. If the denial was not appropriate, the licensed health care professional who acts as the reviewer shall refer the request to **[NAME OF ORGANIZATION]**'s Privacy Officer for action.
4. If access is denied to any portion of the PHI, access must still be granted to those portions of the PHI that are not restricted.
5. **[NAME OF ORGANIZATION]** is bound by the decision of the reviewer.

Provision of Access and Fees

If **[NAME OF ORGANIZATION]** provides a patient or legal representative with access, in whole or in part, to protected health information, **[NAME OF ORGANIZATION]** must comply with the specifications as outlined in the HIPAA privacy regulations and as identified in **[NAME OF ORGANIZATION]**'s Notice of Privacy Practices.

[NAME OF ORGANIZATION] shall provide the access requested in a timely manner and arrange for a mutually convenient time and place for the patient to inspect the PHI or obtain copies, unless access by another method has been requested by the patient and agreed to by **[NAME OF ORGANIZATION]** as set forth above. Any requests for accommodations shall be sent or given in writing to **[NAME OF ORGANIZATION]**'s Privacy Officer.

If the individual requests a copy of the protected health information or agrees to a summary or explanation of such information a reasonable, cost-based fee will be imposed. The fee should only include the cost of copying, including the cost of supplies for and labor of copying, the protected health information and postage if applicable.

Definitions See glossary for key terms and acronyms used in this policy.

Enforcement Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

Rationale/Source This policy complies with requirements of the following:

- Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations Section 164.524

Cross References For additional information, refer to the following:

Document Name

Review or Revision Date This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Privacy Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR ACCOUNTING OF DISCLOSURES

[Insert Logo or Organization Name]

Corporate Privacy Policy

Dates: **Latest Revision:** April 14, 2003
 Original Effective Date:

Replaces:

Purpose

The purpose of this policy is to provide management and workforce members with a standard procedure for accounting of all disclosures of patients protected health information.

Policy

Our organization will maintain a detailed accounting of all disclosures of Patient's Health Information by utilizing a Disclosure Log within each Medical Record. The organization will provide one free accounting per 12-month period. For each additional request by a patient within that period, our standard fee is \$. Our Policy is to review all requests for disclosure and provide a detailed accounting of disclosures to the patient within sixty-days (60) from the date of the request.

Procedure

Create and insert a **Form for Accounting of Health Disclosures** in the patient's medical record/file and document each instance where the health information is disclosed. Include a brief summary of the purpose for disclosure so that the patient will be reasonably informed.

For multiple disclosures to the same recipient pursuant to a single authorization under or for a single purpose, summarize the series of disclosures by providing the information otherwise required above for the first disclosure in the series during the accounting period; the frequency, periodicity, or number of disclosures made during the accounting period; and the date of the most recent disclosure in the series.

Ensure that there is a copy of the individual's authorization or a copy of a written request for disclosure corresponding to each line item with the log sheet.

Summarize any entries on the **Form for Accounting of Health Disclosures** indicating disclosures to health oversight agencies/law enforcement, or, made to your organization's professional liability carrier.

If a patient requests an Accounting of Disclosures a detailed report must be provided no later than sixty-days (60) after receipt of the request. If it is not feasible to meet the sixty-day deadline, you may extend the deadline by no more than thirty-days by informing the individual in writing, within the standard sixty-day period, of the reason for the delay. This deadline may be extended once per accounting.

Each accounting made to patients will be tracked on the **Form for Accounting of Health Disclosures** by indicating the date of the accounting (and the purpose of the disclosure - "accounting").

The organization will provide one free accounting per twelve-month period. For each additional request by a patient within that period, a cost-based fee of \$ will be assessed.

Definitions See glossary for key terms and acronyms used in this policy.

Enforcement Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

Rationale/Source This policy complies with requirements of the following:

- Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations

Cross References For additional information, refer to the following:

Document Name
Request for Accounting Disclosures Form
Form for Accounting of Health Disclosures

Review or Revision Date This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Privacy Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR HEALTH RECORD AMENDMENT

[Insert Logo or Organization Name]

Corporate Privacy Policy

Dates: **Latest Revision:** April 14, 2003
Original Effective Date:

Replaces:

Purpose The purpose of this policy is to provide management and workforce members with a standard procedure to patients requesting an amendment to their protected health information.

Policy Patients who believe information in their health records is incomplete or incorrect may request an amendment or correction to the information as outlined below:

Procedure The patient may approach the author of the entry, point out the error, and ask the author to correct it.

The entry author can correct the entry or add a progress note to clarify content.

The Privacy Officer will assist the patient in completing the health record correction/amendment form.

Upon completion of the form, the Privacy Officer will give a copy of the form to the patient, place a copy in the patient's health record immediately, and route the original and first copy with the record to the author.

If the author chooses to add a comment to the amendment/correction form, the second copy of the form will be routed to the patient with the author's comments.

The original correction/amendment with the author's signature will replace the copy previously placed in the patient's record.

Copies of the correction/amendment form will be furnished to those individuals or organizations the patient deems necessary and documents on the correction/amendment form.

Copies of the correction/amendment form will also be furnished to the facility's business associates or others who have the information subject to the amendment.

Disclosures will be noted on the correction/amendment form with a short notation indicating to whom the correction/amendment form was sent, the date, and the staff member processing the disclosure.

Procedure When a correction/amendment form is used, the Privacy Officer will make an entry at the site of the information that is being corrected or amended indicating, "See correction/amendment," and will date and sign that entry. The correction/amendment form will be attached to the incorrect or amended entry.

Whenever a copy of the corrected/amended entry is disclosed, a copy of the correction/amendment form will accompany the disclosed entry.

Definitions See glossary for key terms and acronyms used in this policy.

Enforcement Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

Rationale/Source This policy complies with requirements of the following:

- Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations Section 164.526(a)(1)

Cross References For additional information, refer to the following:

Document Name
<ul style="list-style-type: none"> • Health Record Amendment Form

Review or Revision Date This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Privacy Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR ACCEPTING AND DENYING RESTRICTIONS OF PHI

[Insert Logo or Organization Name]

Corporate Privacy Policy

Dates: **Latest Revision:** April 14, 2003

Replaces: **Original Effective Date:**

Purpose The purpose of this policy is to provide management and members of the workforce with a standard procedure for restricting access to patient's protected health information.

Policy If a patient wishes to request a restriction on the use or disclosure of Health Information ensure that the patient completes a PATIENT REQUEST FOR RESTRICTIONS OF PHI. Each request is handled and reviewed on a case-by-case basis; however, it is the standard practice of [NAME OF ORGANIZATION] to deny requests that interfere with treatment, payment, or operations.

Procedure Before approving this request appropriate considerations will be given to the need to access PHI for treatment purposes. If the restriction may interfere with treatment it is our standard policy to discuss this with the patient and only agree to restrictions that will not interfere with the patient's treatment.

Any agreed upon restrictions will be documented in the **Form for Accounting of PHI Disclosures**. The documentation will be retained for six (6) years from the date it was last in effect to comply with the HIPAA Privacy Regulations.

Information use and disclosure must remain consistent with any agreed-upon restrictions.

A restriction set by a patient can only be terminated with the patient's written or oral agreement. It is the standard of our organization to require a signature approving the termination of any authorization.

The date that the restriction is terminated must be documented ("End Date") on the **Form for Accounting of PHI Disclosures**.

Definitions See glossary for key terms and acronyms used in this policy.

Enforcement Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

**Rationale/
Source**

This policy complies with requirements of the following:

- Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations
-

**Cross
References**

For additional information, refer to the following:

Document Name
Patient Request Form Restrictions of PHI
Disclosures of PHI Log Sheet

**Review or
Revision Date**

This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance

Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Privacy Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR MINIMUM NECESSARY USES AND DISCLOSURES OF PHI

[Insert Logo or Organization Name]

Corporate Privacy Policy

Dates: **Latest Revision:** April 14, 2003
Original Effective Date:

Replaces:

Purpose

The purpose of this policy is to provide management and workforce members with a standard procedure for keeping health information on a need-to-know basis and maintaining the confidentiality patient's medical history.

Policy

When using or disclosing protected health information our organization will make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

Procedure

Access to PHI within this organization is granted on a need-to-know basis. Certain job responsibilities require access to more detailed information than others. It is your responsibility to maintain the confidentiality of this information and not share it with others that do not need it to carry out the duties of their job responsibilities. Your specific level of access to health information **will be identified and documented in your employee confidentiality agreement**. Access to an entire medical record will not be allowed except when justification for use of the entire medical record is specifically identified and documented.

Disclosures of health information to our patients, who are the subject of the health information, do not need to be restricted to minimum necessary. In addition, disclosures authorized by patients are exempt from the minimum necessary requirements unless the authorization to disclose PHI is requested by our organization for its own purposes.

If PHI is requested from another health care practitioner or a health plan (or clearinghouse) on a routine or recurring basis, the requests must be limited to only the reasonably necessary information identified on the chart.

For all other requests, the **privacy officer** will determine what information is reasonably necessary for disclosure on a case-by-case basis.

Definitions

See glossary for key terms and acronyms used in this policy.

Enforcement Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

Rationale/Source This policy complies with requirements of the following:

- Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations (§ 164.514(d))

Cross References For additional information, refer to the following:

Document Name
Policy for General Uses and Disclosures of PHI
Policy for Access to PHI by Workforce Members

Review or Revision Date This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Privacy Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR USE AND DISCLOSURE OF PSYCHOTHERAPY NOTES

[Insert Logo or Organization Name]

Corporate Privacy Policy

Dates: **Latest Revision:** April 14, 2003

Replaces: **Original Effective Date:**

Purpose

The purpose of this policy is to provide information for management and workforce members regarding the use and disclosure of a patient's psychotherapy notes.

Policy

It is the policy of [NAME OF ORGANIZATION] to not allow patients the right to inspect or obtain a copy of psychotherapy notes. A patient may not request a review of an originator's denial of access to psychotherapy notes. However, a patient may be provided access to a summary of the psychiatric treatment.

Procedure

[NAME OF ORGANIZATION] may not release psychotherapy notes, except in specific situations or as required by law.

Psychotherapy notes (i.e., process notes) shall be maintained separately from the medical record.

Summary information (i.e., progress notes) such as current state of the patient, symptoms, summary of the theme of the psychotherapy session, diagnoses medications prescribed, side effects, and other information needed for treatment or payment shall be placed in the medical record.

Authorization for the disclosure of psychotherapy notes is not required in the following circumstances:

1. For use by the originator for treatment;
2. For use in educational programs involving practicing counseling;
3. To defend a legal action brought by the patient;
4. For purposes of the Department of Health and Human Services in determining compliance with the privacy rule;
5. As otherwise required by law; or
6. By a health oversight agency for a lawful purpose related to oversight of a psychotherapist;

Definitions

See glossary for key terms and acronyms used in this policy.

Enforcement Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

Rationale/Source This policy complies with requirements of the following:

- Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations

Cross References For additional information, refer to the following:

Document Name

Review or Revision Date This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Privacy Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR USE AND DISCLOSURE OF PHI FOR MARKETING

[Insert Logo or Organization Name]

Corporate Privacy Policy

Dates: **Latest Revision:** April 14, 2003

Replaces: **Original Effective Date:**

Purpose

The purpose of this policy is to establish guidelines for management and workforce members regarding the use and disclosure of a patient's protected health information (PHI) for marketing.

Policy

[NAME OF ORGANIZATION]'s employees and workforce members may not disclose, use, sell or coerce an individual to consent to the disclosure, use, or sale of PHI for marketing purposes without the consent or authorization of the patient or representative who is the subject of the PHI. This prohibition includes the disclosure, use or selling of prescription drug patterns. [NAME OF ORGANIZATION]'s employees and workforce members shall not disclose identifiable information such as policy numbers or similar access data codes from a patient's policy or transaction account to any non-affiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer unless the patient has authorized the disclosure.

Certain marketing activities, as described below, do not require [NAME OF ORGANIZATION] to obtain patient authorization for the use or disclosure of PHI.

[NAME OF ORGANIZATION] may use and disclose PHI without obtaining an authorization from the patient to:

1. Provide information on health related products and services in a face-to-face encounter with the patient;
2. Provide information on common health care communications, such as disease management, wellness programs, prescription refill reminders and appointment notifications;
3. Provide the patient with information on participating providers or plans in a network or alternative treatment options;
4. Provide sample products to the patient; and
5. Provide marketing communication involving promotional gifts of nominal value (e.g. calendars, key chains, etc. that promotes [NAME OF ORGANIZATION] or a health care manufacturer's products or services).

If the marketing communication is not face-to-face but in written form, [NAME OF ORGANIZATION] must make a determination prior to sending out the marketing communication that the product or service being marketed may be beneficial to the

health of the patient. In addition, **[NAME OF ORGANIZATION]** is required to send envelopes to the patient that has only the addresses of the sender and the recipient and must:

1. State the name and phone number of **[NAME OF ORGANIZATION]** or the **[NAME OF ORGANIZATION]** affiliated entity sending the marketing information,
2. Explain clearly the recipient’s right to have his/her name removed from the sender’s mailing list,
3. If **[NAME OF ORGANIZATION]** or a **[NAME OF ORGANIZATION]** affiliate for marketing purposes receives a patient’s request for removal from the mailing list, such removal must occur immediately, within FIVE days of receipt of request, and
4. **[NAME OF ORGANIZATION]** must explain in the communication why the patient has been targeted and how the product or service relates to their health.

Definitions See glossary for key terms and acronyms used in this policy.

Enforcement Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

Rationale/Source This policy complies with requirements of the following:

- Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations Section 164.514

Review or Revision Date This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Privacy Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR USE AND DISCLOSURE OF PHI FOR JUDICIAL PROCEEDINGS

[Insert Logo or Organization Name]

Corporate Privacy Policy

Dates: **Latest Revision:** April 14, 2003
Original Effective Date:
Replaces:

Purpose

The purpose of this policy is to provide guidance for management and workforce members regarding the use and disclosure of a patient's protected health information (PHI) judicial and administrative proceedings.

Policy

It is the policy of [NAME OF ORGANIZATION] to permit uses and disclosures of protected health information for judicial or administrative proceedings if the use or disclosure is made in response to a court order, administrative tribunal order, subpoena, discovery request, or other lawful process, without obtaining a patient's written authorization.

Procedures

[NAME OF ORGANIZATION] may use or disclose PHI in the course of any judicial or administrative proceeding if:

1. The disclosure is in response to an order of a court or administrative tribunal, provided that [NAME OF ORGANIZATION] discloses only the PHI expressly authorized by such order; or
2. In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal (such as a subpoena), if:
 - A. [NAME OF ORGANIZATION] receives satisfactory assurance from the party seeking the information that reasonable efforts have been made to ensure that the subject of the requested PHI has been given notice of the request (with an affidavit from the requesting party); or
 - B. [NAME OF ORGANIZATION] receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of this section (in Definitions above).
3. [NAME OF ORGANIZATION] receives satisfactory assurances from a party seeking PHI along with a written statement and accompanying documentation demonstrating that:

- A. The party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);
 - B. The notice included sufficient information about the litigation or proceeding in which the PHI is requested to permit the individual to raise an objection to the court or administrative tribunal; and
 - C. The time for the individual to raise objections to the court or administrative tribunal has elapsed, and:
 - D. No objections were filed; or
 - E. All objections filed by the individual have been resolved by the court or the
 - F. administrative tribunal and the disclosures being sought are consistent with such resolution.
4. **[NAME OF ORGANIZATION]** receives satisfactory assurances from a party seeking PHI including a written statement and accompanying documentation demonstrating that:
 - G. The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or
 - H. The party seeking the PHI has requested a qualified protective order from such court or administrative tribunal.
 5. Notwithstanding this section, **[NAME OF ORGANIZATION]** has the option to disclose PHI in response to lawful process without receiving full satisfactory assurance, if **[NAME OF ORGANIZATION]** of its own accord makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of this section or to seek qualified protective order.

Definitions See glossary for key terms and acronyms used in this policy.

Enforcement Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

Rationale/Source This policy complies with requirements of the following:

- Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations Section 164.512(e)

**Cross
References**

For additional information, refer to the following:

Document Name

**Review or
Revision Date**

This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance

Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Privacy Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR USE AND DISCLOSURE OF PHI TO DHHS (DEPARTMENT OF HEALTH AND HUMAN SERVICES)

[Insert Logo or Organization Name]

Corporate Privacy Policy

Dates: **Latest Revision:** April 14, 2003

Replaces: **Original Effective Date:**

Purpose

The purpose of this policy is establish guidelines for management and workforce members regarding the use and disclosure of a patient's protected health information (PHI) to the Department of Health and Human Services (DHHS).

Policy

It is the policy of **[NAME OF ORGANIZATION]** to permit disclosures of health information to the Department of Health and Human Services (HHS), if necessary, to determine whether **[NAME OF ORGANIZATION]** is in compliance with the HIPAA privacy standards.

DHHS may investigate complaints filed by workforce members and patients. Such investigation may include a review of the pertinent policies, procedures, or practices of **[NAME OF ORGANIZATION]** and of the circumstances regarding any alleged acts or omissions concerning compliance.

DHHS may conduct compliance reviews to determine whether **[NAME OF ORGANIZATION]** is complying with the required HIPAA privacy standards.

[NAME OF ORGANIZATION] will keep records and upon request of DHHS submit compliance reports whereby DHHS can ascertain whether **[NAME OF ORGANIZATION]** has complied with the HIPAA privacy standards.

During an investigation or compliance review, **[NAME OF ORGANIZATION]** will cooperate with DHHS and permit access to information. **[NAME OF ORGANIZATION]** will permit access by DHHS during normal business hours to its books, records, accounts, and other sources of information, including PHI, that are pertinent to ascertaining compliance with the requirements. If DHHS determines that serious circumstances exist, **[NAME OF ORGANIZATION]** will permit access by DHHS at any time and without notice.

If any information required of **[NAME OF ORGANIZATION]** is in the exclusive possession of any other health care provider, agency, institution, or person and the health care provider, agency, institution, or person fails or refuses to furnish the information, **[NAME OF ORGANIZATION]** will document the efforts it has made to obtain the information.

Definitions

See glossary for key terms and acronyms used in this policy.

Enforcement Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

Rationale/Source This policy complies with requirements of the following:

- Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations Section 164.502(a)(2)(ii)

Cross References For additional information, refer to the following:

Document Name
Policy for Violations of Internal Policies

Review or Revision Date This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Privacy Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR EDUCATING AND TRAINING MEMBERS OF THE WORKFORCE

[Insert Logo or Organization Name]

Corporate Privacy and Security Policy

Dates: **Latest Revision: April 14, 2003**
Original Effective Date:
Replaces:

Purpose

The purpose of this policy is to provide guidance for management and workforce members regarding mandatory workforce training as required by the Health Insurance Portability and Accountability Act (HIPAA).

Policy

All workforce members of **[NAME OF ORGANIZATION]**, including staff, volunteers, students, interns and contract employees in **[NAME OF ORGANIZATION]'s** facility on a regular course of business, shall attend training on the privacy and security provisions of HIPAA. This training shall follow a specific curriculum established by **[NAME OF ORGANIZATION]**.

Procedure

Employees and workforce members, including staff, volunteers, students, interns and contract employees in **[NAME OF ORGANIZATION]'s** facility on a regular course of business shall receive HIPAA privacy and security training.

All new employees and workforce members, including staff, volunteers, students, interns and contract employees shall undergo training as part of their initial employee orientation. HIPAA training for new employees must take place within 14 days of the date of hire.

HIPAA training curriculum must remain consistent organization-wide to assure appropriate implementation of the HIPAA privacy and security regulations

- Trainings shall be conducted at the **[NAME OF ORGANIZATION]'s** facility.
- Additional mandatory privacy training shall be scheduled every six months or whenever there is a material change in **[NAME OF ORGANIZATION]'s** privacy policies or procedures as determined by **[NAME OF ORGANIZATION]'s** Privacy Officer.
- Periodic mandatory security training shall be scheduled every six months.

If applicable, each manager at each branch facility of [NAME OF ORGANIZATION] shall identify group(s) or individuals who, due to the nature of their job function, will require in-depth training related to HIPAA, and that specialized training shall be provided by [NAME OF ORGANIZATION]'s Privacy Officer.

Documentation of Mandatory Training

Mandatory HIPAA training shall be documented and maintained for as long as the workforce member is affiliated or employed by [NAME OF ORGANIZATION].

Definitions See glossary for key terms and acronyms used in this policy.

Enforcement Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

Rationale/ Source This policy complies with requirements of the following:
 • Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations Section 164.530(b)(1)

Cross References For additional information, refer to the following:

Document Name

Review or Revision Date This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Privacy Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR DISCLOSURES TO BUSINESS ASSOCIATES

[Insert Logo or Organization Name]

Corporate Privacy and Security Policy

Dates: **Latest Revision:** April 14, 2003

Replaces: **Original Effective Date:**

Purpose

The purpose of this policy is to provide management and workforce members with procedures and protocols that must be followed by management and workforce members regarding disclosures to business associates.

Policy

It is the practice of [NAME OF ORGANIZATION] to utilize third party vendors to perform activities and provide services that involve the use and/or disclosure of protected health information. Vendors that perform activities involving protected health information are labeled “Business Associates.” A business associate is not an employee of [NAME OF ORGANIZATION].

It is the policy of [NAME OF ORGANIZATION] to obtain written assurances from business associates that they will maintain the confidentiality and security of our organization’s protected health information. [NAME OF ORGANIZATION] is required to act if it becomes aware of a practice or pattern that constitutes a material breach of this policy.

Procedure

All personnel must strictly observe the following standards relating to business associates:

[NAME OF ORGANIZATION] must enter into contracts with business associates that contain specific language.

The contract must include language that provides that the business associate will:

Not use or further disclose the information other than as permitted or required by the contract or as required by law;

Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract;

Report to [NAME OF ORGANIZATION] any use or disclosure of the information not provided for by its contract of which it becomes aware;

Ensure that any agents, including any subcontractors, to whom it provides PHI received from, or created by, or on behalf of [NAME OF ORGANIZATION], agree to the same restrictions and conditions that apply to the business associate with respect to such information;

Make available PHI in accordance with the [NAME OF ORGANIZATION]’s Policy for the Inspection of PHI by Individuals;

Make available PHI for amendment and incorporate any amendments to PHI in accordance with the **[NAME OF ORGANIZATION]'s** Policy for Health Record Amendment;

Make available the information required to provide an accounting of disclosures in accordance with the **[NAME OF ORGANIZATION]'s** Policy for Accounting of PHI Disclosures;

Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created by or on behalf of **[NAME OF ORGANIZATION]**, available to DHHS for purposes of determining **[NAME OF ORGANIZATION]'s** compliance; and

At termination of the contract, if feasible, return or destroy all PHI received from, or created by or on behalf of, **[NAME OF ORGANIZATION]** that the business associate still maintains in any form and retain no copies of such information. If such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

In the event **[NAME OF ORGANIZATION]** becomes aware of a pattern or practice of the business associate that constitutes a material breach or violation of the business associate's obligations under its contract, **[NAME OF ORGANIZATION]** must take reasonable steps to cure the breach or to end the violation, as applicable.

In the event that the business associate can not or will not remedy the practice or pattern, **[NAME OF ORGANIZATION]** must terminate the contract if feasible. Where termination is not feasible, contact the **[NAME OF ORGANIZATION]** Privacy Official for reporting to DHHS, as required.

Definitions See glossary for key terms and acronyms used in this policy.

Enforcement Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

**Rationale/
Source** This policy complies with requirements of the following:
Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations
Section
45 C.F.R. §164.314
45 C.F.R. §164.502(e)(1)
45 C.F.R. §160.103

**Cross
References** For additional information, refer to the following:

Document Name
Business Associate Contract General Uses and Disclosures of PHI

**Review or
Revision Date**

This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance

Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Privacy Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR MITIGATION AFTER IMPROPER USE OR DISCLOSURE OF PHI

[Insert Logo or Organization Name]

Corporate Privacy Policy

Dates: **Latest Revision:** April 14, 2003
Original Effective Date:
Replaces:

Purpose The purpose of this policy is to provide procedure to management and workforce members for mitigating the harmful effects of a use or disclosure of protected health information that violates the policies and procedures of the organization.

Policy To the extent practicable, [NAME OF ORGANIZATION] will mitigate any harmful effect that becomes known to [NAME OF ORGANIZATION] as a result of a use or disclosure of PHI in violation of HIPAA or other state health privacy laws or [NAME OF ORGANIZATION] policies and procedures.

Procedure Privacy Officer of [NAME OF ORGANIZATION] shall be responsible for taking corrective measures to remedy violations to the organization's policies and procedures.

If a violation is a result of an employee's negligence or failure to follow [NAME OF ORGANIZATION]'s policies or procedures actions to re-train, reprimand, or discipline the workforce member will be taken immediately.

If a violation is a result of negligence by a business associates the incident should be formally documented and the business associate should provide written assurances indicate the corrective measures that have been taken to remedy the violations.

In the event of an infraction, breach or violation to a patient's protected health information the patient should be notified in writing of the violation and the corrective actions taken to further protect the individual's privacy.

Definitions See glossary for key terms and acronyms used in this policy.

Enforcement Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

Rationale/Source This policy complies with requirements of the following:

- Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations Section 164.530(f)

**Cross
References**

For additional information, refer to the following:

Document Name
Policy for Violations of Internal Policies

**Review or
Revision Date**

This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance

Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Privacy Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR NON-RETALIATION AGAINST EMPLOYEES

[Insert Logo or Organization Name]

Corporate Privacy Policy

Dates: **Latest Revision: April 14, 2003**

Replaces: **Original Effective Date:**

Purpose

The purpose of this policy is to provide procedures for management and workforce members regarding non-retaliation in cases involving the reporting of violations or infractions of HIPAA or other federal or state laws or regulatory requirements.

Policy

All **[NAME OF ORGANIZATION]** workforce members and employees shall be allowed to freely discuss and raise questions to **[NAME OF ORGANIZATION]'s** Privacy Officer or to the appropriate personnel about situations they feel are in violation of HIPAA and other federal and state laws, **[NAME OF ORGANIZATION]'s** policies, and/or accreditation and regulatory requirements.

All **[NAME OF ORGANIZATION]'s** workforce members and employees have a personal obligation to report any activity that appears to violate HIPAA or other applicable laws, regulations, rules, policies, and procedures.

[NAME OF ORGANIZATION] shall not intimidate, threaten, coerce, discriminate against, or take any retaliatory action against the following individuals or in the following situations:

Any patient, legally authorized representative, employee, workforce member, volunteer, associate, association, contractor, organization or group that in good faith:

- (1) Discloses or threatens to disclose information about a situation they feel is inappropriate, or potentially illegal;
- (2) Provides information to or testifies against the alleged offending individual or **[NAME OF ORGANIZATION];**
- (3) Objects to or refuses to participate in an activity they feel are in violation of HIPAA or any other federal and state law, **[NAME OF ORGANIZATION]'s** policies, or accreditation requirements;
- (4) Is involved in any compliance review or peer review process; or
- (5) Files a valid or legitimate report or a complaint, or an incident report.

Procedure All allegations, complaints, violations and incident reports should be formally documented and provided to the Privacy Officer in writing.

[NAME OF ORGANIZATION]’s Privacy Officer will review any allegation of retaliation and will ensure that a proper investigation is conducted as appropriate. The investigation will be in accordance with the **[NAME OF ORGANIZATION]’s Policy for Sanctioning and Disciplining Employees**.

Definitions See glossary for key terms and acronyms used in this policy.

Enforcement Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

Rationale/ Source This policy complies with requirements of the following:

- Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations Section 164.530(g)

Cross References For additional information, refer to the following:

Document Name
Policy for Sanctioning and Disciplining Employees

Review or Revision Date This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Privacy Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR SECURING ELECTRONIC HEALTH INFORMATION

[Insert Logo or Organization Name]

Corporate Security Policy

Dates: **Latest Revision:** April 14, 2003

Replaces: **Original Effective Date:**

Purpose

The purpose of this policy is to provide guidance for management and workforce members in establishing practices which secure protected health information in electronic forms.

Policy

It is the policy of [NAME OF ORGANIZATION] that appropriate measures be taken to secure all individually identifiable health information in electronic formats. Individually Identifiable Health Information shall be labeled "Protected Health Information" and standard procedures must be followed when accessing or maintaining this information over [NAME OF ORGANIZATION]'s information systems.

Procedure

Access to [NAME OF ORGANIZATION] networks from public networks shall be protected by access control systems such as firewalls, access control lists, and user authentication under the observation of designated IT staff or a third party technology vendor.

All network users shall be automatically logged off their workstations after a maximum period of 15 minutes of inactivity.

The Chief Security Officer shall review an audit trail of all accesses and changes to patient data on a regular basis and report violations to employee supervisors and other appropriate staff.

Designated [NAME OF ORGANIZATION] IT staff shall back up data nightly to backup tapes and backup [NAME OF ORGANIZATION] databases in their entirety nightly. Patient information and other data shall be backed up incrementally nightly and fully once a week.

Designated [NAME OF ORGANIZATION] IT shall ensure that all media has been thoroughly cleansed of any patient data before the media is disposed of.

Access to media containing patient data shall be controlled, by designated IT staff through:

1. Access control lists to network media
2. Physical access control to **[NAME OF ORGANIZATION]'s** hardware
3. Purging **[NAME OF ORGANIZATION]'s** data on any type of media before it is discarded
4. Storage of data on media that is backed up

Virus protection for the **[NAME OF ORGANIZATION]'s** network or computer systems shall be maintained by designated staff or technology vendor, pursuant to the following virus protection procedures:

1. All **[NAME OF ORGANIZATION]'s** email servers shall be protected using email-specific anti-virus software.
2. All network and member servers shall be protected using anti-virus software.
3. All workstations, laptops, PDAs or any other device that connects to the **[NAME OF ORGANIZATION]'s** network shall be protected using anti-virus software for that device and installed by designated IT staff.

Equipment that has not been purchased by **[NAME OF ORGANIZATION]** shall only be allowed to connect to the **[NAME OF ORGANIZATION] 's** network upon approval of the Security Officer or designated manager.

Virus Signature Updates

Anti-virus server software shall be configured by designated IT staff to check for virus signature updates daily.

Software Updates

Anti-virus software shall be kept by designated IT staff at the current release or no more than one release below the most current release version.

Software Support

[NAME OF ORGANIZATION] IT staff shall maintain a support contract with the anti-virus software vendor(s) to ensure uninterrupted support.

Attachments

To avoid potentially virus-carrying attachments, **[NAME OF ORGANIZATION] 's** workforce shall not allow certain types of attachments, such as executable and JPEG files to pass through email.

[NAME OF ORGANIZATION] workstations shall be situated by respective designated IT staff to prevent more than incidental observation of work product.

Enforcement Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

Rationale/Source This policy complies with requirements of the following:

- Health Insurance Portability and Accountability Act (HIPAA) Security Regulations Section 164.310(b)

Cross References For additional information, refer to the following:

Document Name
Policy for Data Access Software/Hardware Use Policy

Review or Revision Date This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Security Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR ACCESS TO PHI BY WORKFORCE MEMBERS

[Insert Logo or Organization Name]

Corporate Security Policy

Dates: **Latest Revision:** April 14, 2003

Replaces: **Original Effective Date:**

Purpose

The purpose of this policy is to provide guidance for management and workforce members regarding access to protected health information and to ensure that they recognize the importance of maintaining the confidentiality, security and integrity of protected health information.

Policy

Access by Workforce Members

[Name of Health Care Provider]'s workforce members shall be granted access to protected health information (PHI), whether written, electronic or verbal in nature, in accordance with the Health Insurance Portability and Accountability Act (HIPAA) and other state and federal laws. Such access shall be limited to the "Minimum Necessary" amount of PHI the employee or workforce member needs to know in order to accomplish their job or task. Communications between workforce members which involve PHI shall also be considered confidential and should not take place in public areas. If it is necessary to conduct such conversations in public areas, reasonable steps shall be taken to assure the confidentiality of the PHI.

Patient PHI should never be removed from [NAME OF ORGANIZATION]'s facility without specific authorization from [NAME OF ORGANIZATION]'s Privacy Officer or designee. [NAME OF ORGANIZATION] shall establish a procedure for how workforce members are to physically access PHI in medical records (i.e. how to sign records in and out and under what conditions, etc.).

If PHI in any form is lost or stolen, [NAME OF ORGANIZATION]'s Privacy Officer or designee should be notified as soon as practical, but no later than 24 hours after the loss is discovered, in order for the Privacy Officer or designee to initiate the mitigation process.

Procedure

Training

[NAME OF ORGANIZATION]'s workforce members shall be informed of their obligations with respect to PHI by mandatory participation in HIPAA Privacy Training as required by the Health Insurance Portability and Accountability Act (HIPAA).

Procedure **Required Confidentiality Agreement**

[NAME OF ORGANIZATION]'s workforce members that receive or maintain PHI shall be required to agree to the protection of such PHI. All workforce members shall sign a confidentiality agreement. A copy of the signed confidentiality agreement shall be maintained in their personnel file.

Visitors

Visitors to **[NAME OF ORGANIZATION]'s** facilities will not be required to sign a confidentiality agreement unless they are providing services to **[NAME OF ORGANIZATION]** and may come in contact with confidential information.

Definitions See glossary for key terms and acronyms used in this policy.

Enforcement Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

Rationale/ Source This policy complies with requirements of the following:

- Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations

Cross References For additional information, refer to the following:

Document Name
Policy for Minimum Necessary
Policy for General Uses and Disclosures

Review or Revision Date This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Security Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR ACCEPTABLE WORKSTATION USE

[Insert Logo or Organization Name]

Corporate Security Policy

Dates: **Latest Revision:** April 14, 2003

Replaces: **Original Effective Date:**

Purpose

The purpose of this policy is to establish guidelines for management and workforce members on the proper functions and physical attributes of the surroundings of workstations that access protected health information.

Policy

It is the policy of [NAME OF ORGANIZATION] to secure all workstations that have access to protected health information. Measures will be taken to limit the access to written and electronic protected health information within each physical workstation.

Procedure

All workstations used for [NAME OF ORGANIZATION]'s business activity, no matter where they are located, must use an access control system approved by [NAME OF ORGANIZATION]. In most cases this will involve password-enabled screen-savers with a time-out-after-no-activity feature and a power on password for the CPU and BIOS. Active workstations are not to be left unattended for prolonged periods of time, where appropriate. When a user leaves a workstation, that user is expected to properly log out of all applications and networks.

Users will be held responsible for all actions taken under their sign-on. Where appropriate, inactive workstations will be reset after a period of inactivity (typically 15 minutes). Users will then be required to re-log on to continue usage. This minimizes the opportunity for unauthorized users to assume the privileges of the intended user during the authorized user's absence.

To maintain the security of protected health information workforce members should implement the following physical security measures to their workstation:

Voicemail Access

Each workforce member should ensure that a mechanism or pin code is in place to prevent unauthorized access to the voicemail system from the workstation.

Desk Drawers

Each workforce member should ensure that desk drawers containing electronic media or patient files are securely locked to prevent unauthorized access.

Electronic Media

Electronic media; including disks, tapes, CD, and tape recordings, should be stored in a secure location and left on or around the workstation.

Procedure **Medical Records and Printed Health Information**
 Medical records, when not in use, should be stored in a lock-able file cabinet. If it is necessary to keep medical records in the workstation the records should be stored in a lockable drawer while unattended.

Computer Systems
 Computer systems should have an automatic log-off or screensaver password to prevent unauthorized access. Computer monitors should be positioned so that patients, and other individuals, can not view any protected health information that

Enforcement Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

Rationale/Source This policy complies with requirements of the following:
 • Health Insurance Portability and Accountability Act (HIPAA) Security Regulations Section

Cross References For additional information, refer to the following:

Document Name

Review or Revision Date This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Privacy Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR ELECTRONIC DATA ACCESS

[Insert Logo or Organization Name]

Corporate Security Policy

Dates: **Latest Revision:** April 14, 2003
Original Effective Date:

Replaces:

Purpose The purpose of this policy is to establish guidelines for management and workforce members regarding the access of electronic protected health information.

Policy It is the policy of [NAME OF ORGANIZATION] to ensure that all members of the workforce have appropriate access to electronic protected health information and to prevent those workforce members who do not have access from obtaining access to electronic protected health information.

Procedure All members of the workforce will be assigned a unique login and password before obtaining access to any protected health information on [NAME OF ORGANIZATION]'s computers or network systems. The password shall be known only to the Network Administrator and the member of the workforce. The Network Administrator will specify the level of access granted to the member of the workforce. Instructions on the level of access permissible should be provided by the organization's Privacy and Security Officers.

[Review to ensure that your organization has implemented these measures]
Each computer connected to the Internet at [NAME OF ORGANIZATION]'s facility is assigned a unique IP address. This IP address will track access through the system.

The organization's firewall will track access to outside internet addresses and will block FTP access to prevent members of the workforce from transmitting electronic protected health information.

Enforcement Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

**Rationale/
Source** This policy meets the requirements of the following:
Health Insurance Portability and Accountability Act (HIPAA) Security Regulations
Section 164.308

**Cross
References** For additional information, refer to the following:

Document Name
Organizational Policies and Procedure for Privacy and Security Workforce Confidentiality Agreement

**Review or
Revision Date**

This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance

Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Security Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR DATA CLASSIFICATION

[Insert Logo or Organization Name]

Corporate Security Policy

Dates: **Latest Revision:** April 14, 2003

Replaces: **Original Effective Date:**

Purpose

The purpose of this data access policy is to provide a system for protecting information that is critical to **[NAME OF ORGANIZATION]**. All employees that interact with confidential information are expected to familiarize themselves with this and follow its guidelines.

Policy

The **[NAME OF ORGANIZATION]'s** data access system has been designed to support the need to know so that information will be protected from unauthorized disclosure, use, modification, and deletion. Utilizing this data access system will facilitate business activities and help keep the costs for information security to a minimum. Without the consistent use of this data access system [name organization] risks loss of customer relationships, loss of public confidence, internal operational disruption, excessive costs, and competitive disadvantage.

Procedure

Applicable Information: This data classification policy is applicable to all information in the **[NAME OF ORGANIZATION]'s** possession. For example, medical records on patients, confidential information from suppliers, business partners and others must be protected with this data classification policy. No distinctions between the word data, information, knowledge, and wisdom are made for purposes of this policy.

Consistent Protection: Information must be consistently protected throughout its life cycle, from its origination to its destruction. Information must be protected in a manner commensurate with its sensitivity, regardless of where it resides, what form it takes, what technology was used to handle it, or what purpose(s) it serves. Although this policy provides overall guidance, to achieve consistent information protection, workers will be expected to apply and extend these concepts to fit the needs of day-to-day operations.

CLASSIFICATION LABELS

Public: This classification applies to information that is available to the general public and intended for distribution outside **[NAME OF ORGANIZATION]'s** office. This information may be freely disseminated without potential harm. Examples include product and service brochures, advertisements, job opening announcements, and press releases.

Procedure

For Internal Use Only: This classification applies to all other information that does not clearly fit into the other classifications. The unauthorized disclosure, modification or destruction of this information is not expected to seriously or adversely impact **[NAME OF ORGANIZATION]'s** business, patients, employees, or business partners. Examples include the company telephone directory, new employee training materials, and internal policy manuals.

Confidential: This classification applies to information that is intended for use within the **[NAME OF ORGANIZATION]'s** practice. Unauthorized disclosure could adversely impact **[NAME OF ORGANIZATION]'s** business, patients, employees and business partners. Information that some people would consider private is included in this classification. Examples include medical information (except that which is restricted confidential), patient medical charts, appointment schedules, patient account records, department financial data, purchasing information, vendor contracts.

Restricted Confidential: This classification applies to the most sensitive medical and business information that is intended strictly for use within the **[NAME OF ORGANIZATION]'s** business. Its unauthorized disclosure could seriously and adversely impact **[NAME OF ORGANIZATION]'s** business, patients, employees and business partners. For example, statutorily protected medical information such as, mental health treatment, HIV testing, sexually transmitted diseases, abortion, and alcoholism or substance abuse treatment data.

Definitions

See glossary for key terms and acronyms used in this policy.

Enforcement

Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

**Rationale/
Source**

This policy complies with requirements of the following:

- Health Insurance Portability and Accountability Act (HIPAA) Regulations

**Cross
References**

For additional information, refer to the following:

Document Name
Policy for Securing Electronic Health Information
Policy for Electronic Data Access

**Review or
Revision Date**

This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Security Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR PASSWORD PROTECTION

[Insert Logo or Organization Name]

Corporate Security Policy

Dates: **Latest Revision:** April 14, 2003

Replaces: **Original Effective Date:**

Purpose

This policy outlines the handling, responsibilities, and scope of passwords for the information systems of the **[NAME OF ORGANIZATION]**.

Policy

Passwords for *all* systems are subject to the following rules:

- No passwords are to be spoken, written, e-mailed, hinted at, shared, or in any way known to anyone other than the user involved. This includes supervisors and personal assistants.
- No passwords are to be shared in order to "cover" for someone out of the office. Contact IT, and it will gladly create a temporary account if there are resources you need to access.
- Passwords are not to be your name, address, date of birth, username, nickname, or any term that could easily be guessed by someone who is familiar with you.
- Passwords are not be displayed or concealed on your workspace.

[Name of Organization]'s password policy will address the passwords for the following IT systems with their rules:

- **Network and client operating system:** Windows 2000 username and password (Users will automatically be prompted at a login to change the password every 45 days.)
- **Outlook/Exchange groupware:** Windows 2000 username and password (Users will automatically be prompted at a login to change the password every 45 days.)
- **Computer BIOS password:** Hardware-level access to your computer (This password will not automatically change.)
- **VPN password:** **[NAME OF ORGANIZATION]**'s telecommuting system (Users will be prompted to change this password once a year.)
- **ERP system:** SAP credentials to the production system (Users will be prompted to change this password once a year.)
- **WWW accounts:** Credentials to external Web resources (These passwords are rarely changed unless initiated by the user. IT has disabled the option for these credentials to be saved [IE password caching] on all **[NAME OF ORGANIZATION]** computers.)

Password composition

The following systems have systematically enforced password requirements as stated:

- Policy**
- Network and client operating system (and Outlook): Passwords must meet the following criteria:
 - Password may not contain all or part of the user's account name.
 - Password is at least six characters long.
 - Password contains characters from three of the following four categories:
 - English uppercase characters (A...Z)
 - English lowercase characters (a...z)
 - Base 10 digits (0...9)
 - Nonalphanumeric (exclamation point [!], dollar sign [\$], pound sign [#], percent sign [%], etc.)

Definitions See glossary for key terms and acronyms used in this policy.

Enforcement Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

Rationale/ Source This policy complies with requirements of the following:

- Health Insurance Portability and Accountability Act (HIPAA) Security Regulations

Cross References For additional information, refer to the following:

Document Name
Policy for the Use of Information Systems

Review or Revision Date This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Security Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR INSTANT MESSAGING

[Insert Logo or Organization Name]

Corporate Security Policy

Dates: **Latest Revision: April 14, 2003**

Replaces: **Original Effective Date:**

Purpose

The purpose of this policy is to establish guidelines for management and workforce members for the appropriate use of instant messaging within the organization.

Policy

It is the policy of **[NAME OF ORGANIZATION]** that communications systems generally must be used only for business activities. Incidental personal use is permissible if required because of an immediate or emergency situation. IM users are forbidden from using **[NAME OF ORGANIZATION]'s** electronic communications systems (including cell phones, pagers, and e-mail) for charitable endeavors, private business activities, or amusement/entertainment purposes unless expressly approved by the Security Officer.

Procedure

Although subject to changes, **[NAME OF ORGANIZATION]** has adopted **[identify IM application here; i.e., only one external commercial instant messaging service: America Online Instant Messenger (AIM)]**.

The overall management of the IM policy, IM usage and monitoring, and IM equipment maintenance are the responsibility of the **[SECURITY OFFICER]**. The **[SECURITY OFFICER]** will coordinate all company-authorized IM installations. Individuals must contact the **[SECURITY OFFICER]** if they wish to request any changes.

Employees must obtain approval prior to using or installing any IM software or hardware, and they must use only the company's internal or external IM client and services to communicate with fellow employees or business associates.

If asked to do so, employees are required to surrender all IM-related material provided for them to the company in a timely matter and discontinue the use of the **[NAME OF ORGANIZATION]**-based username.

Use only the company's internal or external IM client and services to communicate with fellow employees or business associates.

- Do not discuss confidential information through any public IM services.
- Do not open or accept IM attachments transmitted through a public IM service. All attachments/files will be sent via the company e-mail system.

Be aware that all IM conversations on the company's network system should not be considered private.

Procedure If you think that your IM username or session has been compromised, shut down your session immediately and call the **Security Officer** as soon as possible. If the compromise occurs after hours, shut down your session as well as your Internet connection and call the **Security Officer** as soon as possible.

Enforcement Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

Rationale/Source This policy complies with requirements of the following:

- Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations

Cross References For additional information, refer to the following:

Document Name
Policy for Electronic Data Access
Policy for the Use of Information Systems

Review or Revision Date This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Privacy Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR ACCEPTABLE USE OF EMAIL

[Insert Logo or Organization Name]

Corporate Security Policy

Dates: **Latest Revision:** April 14, 2003

Original Effective Date:

Replaces:

Purpose

The purpose of this policy is to define appropriate standards for management and workforce members for secure and effective use of the electronic mail system within the organization.

Policy

[NAME OF ORGANIZATION] forbids the use of company electronic communications resources for any purpose that could reveal individually identifiable health information or compromise confidential information. The company also forbids electronic communications that interfere with the use of these resources by other employees.

Electronic mail is intended to be used as a business tool to facilitate communications and the exchange of information needed to perform an employee's job. Incidental personal use is permissible so long as: (a) it does not consume more than a trivial amount of resources, (b) does not interfere with worker productivity, and (c) does not preempt any business activity.

Users have an obligation to use e-mail appropriately, effectively, and efficiently.

Users must be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed and stored by others. Therefore, users must utilize discretion and confidentiality protections equal to or exceeding that which is applied to written documents.

E-mail should not be used for urgent or time-sensitive communications.

Business e-mail accounts and passwords should not be shared or revealed to anyone else besides the authorized user(s).

Prohibited Uses

Use of electronic mail is to be in compliance with all applicable state and federal statutes and **[NAME OF ORGANIZATION]'s** policies and procedures. Prohibited usage of the Company's electronic mail system includes, but is not limited to:

- Copying or transmission of any document, software or other information protected by copyright and/or patent law, without proper authorization by the copyright or patent owner;

- Engaging in any communication that is threatening, defamatory, obscene, offensive, or harassing.
- Use of e-mail system for solicitation of funds, political messages, gambling, commercial, or illegal activities
- Disclosure of an individual's personal information without appropriate authorization
- Transmission of information to individuals inside or outside the company without a legitimate business need for the information.
- Use of e-mail addresses for marketing purposes without explicit permission from the target recipient.
- Transmission of highly confidential or sensitive information, e.g., HIV status, mental illness, chemical dependency and workers compensation claims.
- Forwarding of e-mail from in-house or outside legal counsel, or the contents of that mail, to individuals outside of the company without the express authorization of counsel.
- Misrepresenting, obscuring, suppressing, or replacing a user s identity on an electronic communication.
- Attempting unauthorized access to data or attempting to breach any security measure on any electronic communication system, or attempting to intercept any electronic communication transmissions without proper authorization.

All users of e-mail systems do so with the understanding that they have no expectation of privacy relating to that use. **[NAME OF ORGANIZATION]'s** reserves the right to access the electronic mail system for the purpose of ensuring the protection of legitimate business interests and proper utilization of its property.

E-Mail Confidentiality

Users of **[NAME OF ORGANIZATION]'s** electronic mail system may have the capacity to forward, print and circulate any message transmitted through the system. Therefore:

Users should utilize discretion and confidentiality protections equal to or exceeding that which is applied to written documents.

- Information considered confidential or sensitive must be protected during transmission of the data utilizing encryption or some other system of access controls that ensure the information is not accessed by anyone other than the intended recipient.
- A notation referring to the confidential or sensitive nature of the information should be made in the subject line.
- Confidential or sensitive information may be distributed to multiple recipients; however, the use of distribution lists is prohibited.
- Confidential or sensitive information is to be distributed only to those with a legitimate need to know.

E-Mail Retention

Generally, e-mail messages constitute temporary communications, which are non-vital and may be discarded routinely. However, depending on the content of an e-mail message, it may be considered a more formal record and should be retained.

Enforcement

Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

Cross Reference

For additional information, refer to the following:

Document Name
Hardware/Software Use Policy

Review or Revision Date

This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance

Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Security Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR TRANSMITTING AND RECEIVING ELECTRONIC PHI

[Insert Logo or Organization Name]

Corporate Security Policy

Dates: **Latest Revision:** April 14, 2003

Replaces: **Original Effective Date:**

Purpose The purpose of this policy is to establish guidelines for management and workforce members regarding the security of electronic transmissions.

Policy It is the policy of [NAME OF ORGANIZATION] to monitor and safeguard all electronic transmissions of protected health information. Electronic transmissions include transactions using all media, transmissions over the Internet (including e-mail), dial-up lines, and private networks.

Procedure Transmitting protected health information electronically is a critical part of [NAME OF ORGANIZATION]'s business operations. It is the business practice of [NAME OF ORGANIZATION] to encrypt and encode all data that is being transmitted outside of [NAME OF ORGANIZATION]'s facility.

Compressed Files

In the course of business it may be necessary to compress data files that contain protected health information. All compressed files that contain protected health information should be encoded with a password. The password should be provided to the recipient over the telephone. This password should not be the same or similar to the password used by workforce members for accessing [NAME OF ORGANIZATION]'s computers or network.

Electronic Mail (E-Mail) Transmittals

In the course of business it may be necessary to send protected health information in an e-mail message for the purposes of treatment, payment or healthcare operations. In these instances encryption should be utilized for safeguarding the integrity and maintaining the confidentiality of the information. The Administrator or Technology director will determine the most efficacious method of encryption within [NAME OF ORGANIZATION] and members of the workforce will be instructed on sending encrypted transmissions.

Electronic Media

In instances where electronic media is being utilized to transmit or transfer protected health information a password should implemented to secure the media. If it is not feasible to password protect the media the sender of the electronic media should obtain verbal and/or written confirmation that the intended recipient has received the electronic media.

Procedure

Dial-Up Lines and Private Networks

In the course of business it may be necessary to transmit or receive electronic protected health information while using a dial-up internet connection or private network outside **[NAME OF ORGANIZATION]'s** network. In these instances workforce members should implement a personal firewall and encryption for data transfers. **If [NAME OF ORGANIZATION] has established a Virtual Private Network (VPN) workforce members should establish their connection through the VPN.**

Enforcement

Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

**Rationale/
Source**

This policy complies with requirements of the following:

- Health Insurance Portability and Accountability Act (HIPAA) Security Regulations 164.312(a)(2)iv and 164.312(c)

**Cross
References**

For additional information, refer to the following:

Document Name
Policy for Password Protection
Policy for Acceptable use of E-mail

**Review or
Revision Date**

This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance

Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Security Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR FAX TRANSMITTAL OF PHI

[Insert Logo or Organization Name]

Corporate Security Policy

Dates: **Latest Revision:** April 14, 2003

Replaces: **Original Effective Date:**

Purpose

The purpose of this policy is to establish guidelines for management and workforce members regarding the transmission and receipt of protected health information by facsimile (fax).

Policy

It is the policy of [NAME OF ORGANIZATION] to protect the facsimile transmittal of PHI and hold individuals responsible for following the proper procedure when PHI is sent via facsimile. [NAME OF ORGANIZATION] protects the confidentiality and integrity of confidential medical information as required by law, professional ethics, and accreditation requirements. This policy defines the minimum guidelines and procedures that must be followed when transmitting patient information via facsimile.

Procedure

All workforce members of [NAME OF ORGANIZATION] must strictly observe the following standards relating to facsimile communications of patient medical records:

PHI will be sent by facsimile only when the original record or mail-delivered copies will not meet the needs for TPO. For example, personnel may transmit PHI by facsimile when urgently needed for patient care or required by a third-party payer for ongoing certification of payment for a patient.

Information transmitted must be limited to the minimum necessary to meet the requester's needs.

A properly completed and signed authorization must be obtained before releasing PHI for purposes other than treatment, payment, or healthcare operations. The following types of medical information are protected by federal and/or state statute and may NOT be faxed or photocopied without specific written patient authorization, unless required by law:

- Confidential details of psychotherapy (records of treatment by a psychiatrist, licensed psychologist or psychiatric clinical nurse specialist).
- Other professional services of a licensed psychologist.
- Social work counseling/therapy.
- Domestic violence victims' counseling.
- Sexual assault counseling.
- HIV test results. (Patient authorization required for EACH release request.)

Procedure

- Records pertaining to sexually-transmitted diseases.
- Alcohol and drug abuse records protected by federal confidentiality rules (42 CFR Part 2)

A "Facsimile Cover Letter" must be used to send faxes containing PHI. All pages plus the cover page of all confidential documents to be faxed must be marked "Confidential" before they are transmitted.

Personnel must make reasonable efforts to ensure that they send the facsimile transmission to the correct destination including:

Preprogramming frequently used numbers into the machine to prevent misdialing errors.

Periodically and/or randomly checking all speed-dial numbers to ensure their currency, validity, accuracy, and authorization to receive confidential information.

For a new recipient, the sender must verify the fax number by requesting the recipient submit a faxed or email request for PHI, which would include the fax number of the recipient.

1. Periodically reminding those who are frequent recipients of PHI to notify **[NAME OF ORGANIZATION]**'s if their fax number is to change.

A copy of the fax transmittal and fax confirmation sheet must be maintained for future reference.

Misdirected Faxes

If a fax transmission containing PHI is not received by the intended recipient because of a misdial, check the fax machine to obtain the misdialed number. If possible, a phone call (supplemented by a note referencing the conversation) should be made to the recipient of the misdirected fax requesting that the entire content of the misdirected fax be destroyed. If the recipient cannot be reached by phone, a fax should be sent directing the recipient to destroy the entire contents of the misdirected fax.

Receipt of Faxes Containing PHI

Fax machines used for patient care or patient related services shall not be located in areas accessible to the general public but rather must be in secure areas, and the Privacy Officer is responsible for limiting access to them.

Receiving Faxes

Faxes should be immediately removed from the fax machine and delivered to the recipient.

Destroy, or follow sender's instructions for patient information faxed in error and immediately inform the sender.

Enforcement Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

Rationale/Source This policy complies with requirements of the following:

- Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations

Cross References For additional information, refer to the following:

Document Name

Review or Revision Date This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Security Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR MEDIA CONTAINING ELECTRONIC PHI

[Insert Logo or Organization Name]

Corporate Security Policy

Dates: **Latest Revision:** April 14, 2003

Replaces: **Original Effective Date:**

Purpose

The purpose of this policy is to establish guidelines for management and workforce members regarding the receipt, removal and storage of hardware and electronic media that contain electronic protected health information.

Policy

It is the policy of [NAME OF ORGANIZATION] to safeguard all electronic media that contains protected health information. Electronic media includes magnetic tapes, disks, optical disks, and digital memory cards. [NAME OF ORGANIZATION] utilizes electronic media for transmitting protected health information and for backup purposes.

The use of outside media brought to the facility by members of the workforce is prohibited. The use of outside media provided by vendors may be used providing it has been approved by the Security Officer.

Procedure

All electronic media should be scanned for viruses before transferring data between the media and [NAME OF ORGANIZATION]'s information systems.

Data backup and storage

[NAME OF ORGANIZATION] performs daily backups of its electronic data. All tapes should be stored in a secure location within [NAME OF ORGANIZATION]'s facility.

Removal of Electronic Media

The removal of electronic media from [NAME OF ORGANIZATION]'s facility is prohibited unless specific approval has been obtained from the Security Officer. A record should be made of the removal of media.

Media Re-Use

In the course of business electronic media may be re-used. Before media may be re-used it should be formatted to prevent unauthorized dissemination of data.

Disposal

In the course of business it may be necessary to dispose of electronic media. Magnetic tapes should be degaussed. Diskettes and memory cards should be destroyed by a third party that specializes in the destruction of electronic media.

Enforcement Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

Rationale/Source This policy complies with requirements of the following:

- Health Insurance Portability and Accountability Act (HIPAA) Security Regulations

Cross References For additional information, refer to the following:

Document Name
Policy for the Use of Information Systems
Policy for Securing Electronic Health Information

Review or Revision Date This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Security Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR MAINTAINING PHYSICAL SECURITY

[Insert Logo or Organization Name]

Corporate Security Policy

Dates: **Latest Revision:** April 14, 2003

Replaces: **Original Effective Date:**

Purpose The purpose of this policy is to establish guidelines for management and workforce members regarding the physical security of **[NAME OF ORGANIZATION]**.

Policy It is the policy of **[NAME OF ORGANIZATION]** to limit physical access to **[NAME OF ORGANIZATION]'s** facility, information systems, medical records and equipment to only authorized personnel.

Procedure Access to **[NAME OF ORGANIZATION]'s** facility should be granted on an as-needed basis. The Security Officer is responsible for identifying the access needed for members of the workforce to carry out the functions of their job.

Medical Record Storage

Medical records maintained at **[NAME OF ORGANIZATION]'s** facility should be locked at the end of each business day. The Privacy Officer should designate (1) individual for monitoring and maintaining the organization's medical records. This individual should be responsible for retrieving records and documenting disclosures.

Equipment Control

Servers and network equipment should be stored in a lockable office or cabinet. Access should be limited to the Network Administrator and/or Security Officer.

Storage of Electronic Media

Electronic media, including diskettes, magnetic tapes, and memory sticks, should be stored in a secure location within the facility. When not in use electronic media should be maintained in a central repository or in lockable desk drawers.

Visitors and Vendors

To prevent unauthorized access all visitors and vendors should sign-in documenting the time and purpose for visit. Individuals receiving treatment should not document their reason for visit.

Enforcement Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

**Rationale/
Source**

This policy complies with requirements of the following:

- Health Insurance Portability and Accountability Act (HIPAA) Security Regulations Section 164.310(1)
-

**Cross
References**

For additional information, refer to the following:

Document Name

**Review or
Revision Date**

This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance

Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Security Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR THE RETENTION OF DOCUMENTATION

[Insert Logo or Organization Name]

Corporate Security Policy

Dates: **Latest Revision:** April 14, 2003

Replaces: **Original Effective Date:**

Purpose

The purpose of this policy is to establish guidelines for management and workforce members regarding the retention and maintenance of documentation created during the HIPAA compliance process.

Policy

This policy defines the guidelines and procedures that must be followed for the retention of any policy, procedure or documentation developed by [NAME OF ORGANIZATION] while implementing the HIPAA privacy and security standards.

Procedure

As required by the HIPAA privacy and security rules [NAME OF ORGANIZATION] will retain all policies and procedures developed by [NAME OF ORGANIZATION] during its implementation of the HIPAA standards and specifications.

[NAME OF ORGANIZATION] will make records and document any activity, action or assessment required by the HIPAA privacy and security rules.

[NAME OF ORGANIZATION] will record and retain any communication required by the HIPAA privacy or security rules.

[NAME OF ORGANIZATION] will retain the required documentation for six years from the date of its creation or the date when it last was in effect, whichever is later.

All documentation and records created for the purpose of compliance with the HIPAA regulations will be stored and recorded in [NAME OF ORGANIZATION]'s HIPAA compliance manual.

Enforcement

Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

Rationale/ Source

This policy complies with requirements of the following:

- Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Regulations

Cross References

For additional information, refer to the following:

Document Name

**Review or
Revision Date**

This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance

Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Security Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR THE DISPOSAL OF PHI

[Insert Logo or Organization Name]

Corporate Security Policy

Dates: **Latest Revision:** April 14, 2003

Replaces: **Original Effective Date:**

Purpose

The purpose of this policy is to provide management and workforce members with the procedures for the proper disposal of protected health information.

Policy

It is the policy of **[NAME OF ORGANIZATION]** to only dispose of protected health information (PHI) by means that assure that it will not be accidentally released to an outside party. This policy is to define the guidelines and procedures that must be followed when disposing of information containing PHI.

Procedure

Destruction of Copies and Original Documentation

1. **[NAME OF ORGANIZATION]** 's Security Officer and supervisor(s) shall provide users with access to shredders or secured recycling bags for proper disposal of confidential printouts containing PHI.
2. Users may elect to use either shredding or secure recycle bags for the destruction of copies, as long as the destruction is in accordance with this policy.

Electronic Copies

1. The Security Officer is responsible for the destruction of electronic copies containing PHI. However, employees may dispose of the electronic data themselves using the following methods:
 - a. Deleting on-line data using the appropriate utilities;
 - b. "Degaussing" computer tapes to prevent recovery of data;
 - c. Removing PHI from mainframe disk drives being sold or replaced, using the appropriate initialization utilities;
 - d. Erasing diskettes to be re-used using a special utility to prevent recovery of data; or
 - e. Destroying discarded diskettes.

Procedure

Printed Material and Hardcopy Data

1. PHI printed material shall be shredded and recycled by a firm specializing in the disposal of confidential records or be shredded by an employee of **[NAME OF ORGANIZATION]** authorized to handle and personally shred the PHI.
2. Microfilm or microfiche must be cut into pieces or chemically destroyed.
3. If hardcopy PHI (paper, microfilm, microfiche, etc.) cannot be shredded, it must be incinerated.

Documentation of Destruction

1. To ensure that it is in fact performed, **[NAME OF ORGANIZATION]** 's personnel or a bonded destruction service must carry out the destruction of PHI.
2. If a bonded shredding company undertakes the destruction, the bonded shredding company must provide **[NAME OF ORGANIZATION]** with the document of destruction that contains the following information:
 - Date of destruction,
 - Method of destruction,
 - Description of the disposed records,
 - Inclusive dates covered,
 - A statement that the records have been destroyed in the normal course of business,
 - The signatures of the individuals supervising and witnessing the destruction
3. The bonded shredding company must provide **[NAME OF ORGANIZATION]**'s Security Officer with a Certificate of Destruction.

Definitions

See glossary for key terms and acronyms used in this policy.

Enforcement

Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

**Rationale/
Source**

This policy complies with requirements of the following:

- Health Insurance Portability and Accountability Act (HIPAA) Security Regulations Section 164.310(d)(2)(i)

**Cross
References**

For additional information, refer to the following:

Document Name

**Review or
Revision Date**

This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance

Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Security Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR REPORTING SECURITY INCIDENTS

[Insert Logo or Organization Name]

Corporate Security Policy

Dates: **Latest Revision:** April 14, 2003

Replaces: **Original Effective Date:**

Purpose

The purpose of this policy is to establish guidelines for management and workforce members for identifying and responding to suspected or known security incidents.

Policy

A security incident is an attempted or successful unauthorized access, use, disclosure, modification, destruction of information, or interference with system operations. It is the policy of [NAME OF ORGANIZATION] that all workforce members notify the Security Officer in the event of a security incident.

Procedure

In the event that a member of the workforce has knowledge of a security incident that may jeopardize the integrity or confidentiality of [NAME OF ORGANIZATION]'s information systems the workforce member is required to immediately notify the Security Officer.

The Security Officer will review logs, audit trails, or relevant documentation that may provide additional information regarding the reported incident. If the security incident is a result of inadequate technical safeguards the Security Officer should take appropriate measures to amend the weakness in [NAME OF ORGANIZATION]'s security procedures. The Security Officer should document the security incident and the corrective actions taken to prevent future incidents.

The Security Officer will mitigate, to the extent practicable, harmful effects of security incidents that are known to the organization and document security incidents and their outcomes.

Enforcement

Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

Rationale/ Source

This policy complies with requirements of the following:

- Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations
-

Cross References

For additional information, refer to the following:

Document Name
Policy for Mitigation After Improper Use or Disclosure of PHI Policy for Security Electronic Health Information

**Review or
Revision Date**

This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance

Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Security Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR PREVENTING AND DETECTING SECURITY VIOLATIONS

[Insert Logo or Organization Name]

Corporate Security Policy

Dates: **Latest Revision:** April 14, 2003
Original Effective Date:

Replaces:

Purpose The purpose of this policy is to establish guidelines for management and workforce members regarding the prevention, detection, and correction of security violations.

Policy It is the policy of [NAME OF ORGANIZATION] to prevent security violations, to the extent practicable, before they occur. Members of the workforce should be aware of the established practices for preventing security violations.

Procedure Preventing security violations requires that all members of the workforce understand and practice the security policies established by [NAME OF ORGANIZATION]. The following mechanisms will be utilized by [NAME OF ORGANIZATION] to prevent security violations:

Outside Equipment

No outside equipment may be plugged into the [NAME OF ORGANIZATION]'s network without written or verbal authorization by the Security Officer.

Electronic Media

No outside electronic media is permitted within [NAME OF ORGANIZATION] without the permission of the Security Officer. In the event that electronic media must be utilized it should scanned for viruses to prevent malicious software attacks .

Authentication

Any user (remote or internal), accessing [NAME OF ORGANIZATION]'s computer systems, software and network systems will be authenticated to prevent unauthorized access.

Workstation Access Control System

All workstations used for [NAME OF ORGANIZATION]'s business activity, no matter where they are located, should require a password before a user can gain access to the workstation. Active workstations are not to be left unattended for prolonged periods of time.

Minimum Necessary Access

Users should only receive access to the minimum applications and privileges required to carry-out the functions of their job.

Procedure

Audit Trails and Logging

Access to confidential information may be logged and audited in a manner that allows the Security Officer to identify the access time, user account, and method of access used.

Firewall

Firewall logs should be reviewed on a regular basis to identify any irregularities or unauthorized access attempts.

Enforcement

Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal. Enforcement of this policy and sanctions for not abiding by it are documented in the **Policy for Sanctioning and Disciplining Employees** and the **Policy for Violations of Internal Policies**.

**Rationale/
Source**

This policy complies with requirements of the following:

- Health Insurance Portability and Accountability Act (HIPAA) Security Regulations Section 164.308(a)(6)(i)

**Cross
References**

For additional information, refer to the following:

Document Name
Policy for the Use of Information Systems
Policy for Security Electronic Health Information

**Review or
Revision Date**

This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance

Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Security Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR VIOLATIONS OF INTERNAL PROCEDURES

[Insert Logo or Organization Name]

Corporate Privacy and Security Policy

Dates: Latest Revision: January 1, 2003

Original Effective Date:

Replaces:

Purpose

The purpose of this policy is to provide information for management and workforce specifying enforcement, penalty, and disciplinary actions that may result from violation of policies regarding the privacy and protection of an individual's protected health information (PHI) and to offer guidelines on how to conform to the required standards.

Policy

All employees and workforce members of [NAME OF ORGANIZATION] must guard against improper uses and disclosures of protected health information.

It is the standard practice of [NAME OF ORGANIZATION] that all employees and workforce members shall undergo training on the organization's policies and privacy practices. Employees must sign that they understand and agree to the organization's policies.

If there is a question whether a use or disclosure of health information is appropriate the Privacy Officer of should be consulted.

Employees that knowingly violate the organization's policies and procedures will be faced with disciplinary action and possible termination.

Neither [NAME OF ORGANIZATION] as an entity nor any [NAME OF ORGANIZATION] employee will intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against:

1. Any individual for exercising any right or participating in any process established under [NAME OF ORGANIZATION]'s policies, including the filing of a complaint with [NAME OF ORGANIZATION] or with DHHS.
2. Any individual or other person for:
 - A. Filing of a complaint with [NAME OF ORGANIZATION] or with DHHS as provided in [NAME OF ORGANIZATION] privacy policies;
 - B. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing relating to [NAME OF ORGANIZATION] policy and procedures; or

- C. Opposing any unlawful act or practice, provided that:
 - i. The individual or other person (including a [NAME OF ORGANIZATION] staff and workforce member) has a good faith belief that the act or practice being opposed is unlawful; and
 - ii. The manner of such opposition is reasonable and does not involve a use or disclosure of an individual's protected health information in violation of [NAME OF ORGANIZATION] policies.

Disclosures by Whistleblowers and Workforce Crime Victims

Employees, workforce members, or business associates of [NAME OF ORGANIZATION] may disclose an individual's protected client information if:

- 1. Employees, workforce members, or business associates of [NAME OF ORGANIZATION] believe, in good faith, that [NAME OF ORGANIZATION] has engaged in conduct that is unlawful or that otherwise violates professional standards or that the care, services, or conditions provided by [NAME OF ORGANIZATION] could endanger employees, workforce members, patients, or the public; and
- 2. The disclosure is to:
 - A. An oversight agency or public authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of [NAME OF ORGANIZATION];
 - B. An appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or of misconduct by [NAME OF ORGANIZATION]; or
 - C. An attorney retained by or on behalf of the employees, workforce members, or business associates of [NAME OF ORGANIZATION] for the purpose of determining the legal options of the employee, workforce member, or business associate with regard to this policy.

Employees and workforce members of [NAME OF ORGANIZATION] may disclose limited protected information about an individual to a law enforcement official if the staff or workforce member is the victim of a criminal act and the disclosure is:

- A. About only the suspected perpetrator of the criminal act; and
- B. Limited to the following information about the suspected perpetrator:
 - 1. Name and address;
 - 2. Date and place of birth;
 - 3. Social security number;
 - 4. ABO blood type and rh factor;
 - 5. Type of any injury;
 - 6. Date and time of any treatment; and
 - 7. Date and time of death, if applicable.

Employees and workforce members who violate [NAME OF ORGANIZATION] policies and procedures regarding the safeguarding of an individual's information are subject to:

- A. Appropriate disciplinary action by [NAME OF ORGANIZATION], up to and including immediate dismissal from employment.
- B. Legal action by the individual who may also want to pursue a tort claim against [NAME OF ORGANIZATION].

[NAME OF ORGANIZATION] staff and workforce members who knowingly and willfully violate state or federal law for improper invasions of personal privacy may be subject to:

- A. Criminal investigation and prosecution, both by the state and by the federal government, depending on the nature of the violation. Federal and state law provides substantial fines and prison sentences upon conviction, depending on the nature and severity of the violation.
- B. Civil monetary penalties that the federal Department of Health and Human Services (DHHS) may impose.

[NAME OF ORGANIZATION]'s Privacy Officer is responsible for enforcing this policy. Individuals who violate this policy are subject to disciplinary action, up to and including termination or dismissal.

**Rationale/
Source**

This policy complies with requirements of the following:
Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations
Section 45 CFR 164.530

**Cross
References**

For additional information, refer to the following:

Document Name
Organizational Policies and Procedure for Privacy and Security
Employee Confidentiality Agreement

**Review or
Revision Date**

This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY
01/01/2003			

Governance

Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Privacy Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR SANCTIONING AND DISCIPLINING EMPLOYEES

[Insert Logo or Organization Name]

Corporate Security Policy

Dates: Latest Revision: April 14, 2003

Original Effective Date:

Replaces:

Purpose

The purpose of this policy is to provide guidance for management and workforce members regarding the disciplinary and dismissal policies and procedures to workforce members when breaches of the HIPAA Regulations or [NAME OF ORGANIZATION]'s policies occur.

Policy

All employees are expected to review and understand their job function, its performance requirements and all business practices, procedures, and standards of conduct established by [NAME OF ORGANIZATION]. Any employee that violates the written policies, procedures, standards of conduct or does not fulfill the duties of their job function, may be subject to disciplinary action.

The Following Conduct May Result in Disciplinary Action:

Work Performance

Failure of an employee to maintain satisfactory work performance standards constitutes good cause for disciplinary action which may include dismissal. The term "work performance" includes all aspects of an employee's work.

- Work performance is judged by the supervisor's evaluation of the quality and quantity of work performed by each employee.
- When, in the opinion of the administrator or supervisor, the employee's work performance is below standard, the administrator or supervisor should take appropriate disciplinary action.

Misconduct

All employees are expected to maintain standards of conduct suitable and acceptable to the work environment. Disciplinary action, which may include dismissal, may be imposed for unacceptable conduct. Examples of unacceptable conduct, as applicable, include but are not limited to:

- Falsification of time sheets, personnel records, or other institutional records.
- Neglect of duties, or wasting time during working hours.
- Misappropriation of [NAME OF ORGANIZATION]'s resources.

Policy

- Improper use or disclosure of a patient's Protected Health Information (PHI).
- Improper storage, copying, printing, and disposal of PHI.
- Creating or developing PHI documents that are greater than the minimum necessary for the specific task.
- Smoking (except in designated areas in **[NAME OF ORGANIZATION]'s** facilities).
- Gambling, including participation in lotteries or any other games of chance on the premises at any time.
- Soliciting, collecting money, or circulating petitions on the premises other than within the rules and regulations of **[NAME OF ORGANIZATION]**.
- Bringing intoxicants or drugs onto the premises of **[NAME OF ORGANIZATION]**, using intoxicants or drugs, having intoxicants or drugs in one's possession, or being under the influence of intoxicants or drugs on the premises at any time.
- Disregard for or failure to adhere to established internal controls.
- Abuse or waste of tools, equipment, fixtures, property, supplies, or goods of **[NAME OF ORGANIZATION]**.
- Creating or contributing to unhealthy or unsanitary conditions.
- Violations of safety rules or accepted safety practices.
- Failure to cooperate with a supervisor or co-worker.
- Impairment of function of work unit, or disruptive conduct.
- Disorderly conduct, horseplay, harassment of other employees (including sexual harassment, or use of abusive or profane language on the premises).
- Fighting, encouraging a fight, or threatening, or attempting to cause or causing injury to another person on the premises.
- Neglect of duty or failure to meet a reasonable and objective measure of efficiency and productivity.
- Theft, dishonesty, or unauthorized use of **[NAME OF ORGANIZATION]'s** property including records and confidential information.
- Creating a condition hazardous to another person on the premises.
- Destroying or defacing **[NAME OF ORGANIZATION]'s** property or

records or the property of a student or employee.

- Refusal of an employee to follow instructions or to perform designated work that may be required of an employee or refusal to adhere to established rules and regulations.
- Repeated tardiness or absence, absence without proper notification to the supervisor or without satisfactory reason, or unavailability for work.
- Violation of policies or rules of **[NAME OF ORGANIZATION]**

Procedure

All incidents that involve the potential for disciplinary action shall be investigated by **[NAME OF ORGANIZATION]'s** administrator, or employee's supervisor or other designated administrative official. If the investigation results in evidence that establishes with reasonable certainty that the employee engaged in conduct which warrants disciplinary action, the administrator or employee's supervisor shall follow the pre-disciplinary review procedures before seeking approval for the proposed disciplinary action.

Pre-Disciplinary Review

An employee shall be informed of the basis for any proposed disciplinary action which may result in demotion, suspension without pay, or dismissal and have an opportunity to respond before a final decision is made to take disciplinary action. The review serves as an opportunity to avoid mistaken decisions to impose discipline and is not intended to definitely resolve the propriety of the disciplinary action being considered.

A pre-disciplinary review should be informal before reaching a final decision to impose discipline, the administrator or supervisor shall:

- Inform the employee, in writing, of the reasons for the proposed disciplinary action, the facts upon which the administrator or supervisor relies, the names of any persons who have made statements about the disciplinary incident, and the content of such statements.
- Give the employee an opportunity to respond to the charges either orally or in writing within a reasonable time and to persuade the administrator or supervisor that the evidence supporting the charges is not true. If the administrator or supervisor is not persuaded that the evidence is untrue, the administrator or supervisor may review the evidence and proposed disciplinary action with **[NAME OF ORGANIZATION]'s** owner or managing partner or other appropriate authority before proceeding to impose the disciplinary penalty.

Procedure Disciplinary Action

Upon completing pre-disciplinary review procedures and obtaining the approval of the appropriate authority, the administrator or supervisor shall inform the employee in writing of the following:

- The specific incident, conduct, course of conduct, unsatisfactory work performance, or other basis for the disciplinary penalty.
- Any previous efforts to make the employee aware of the need to change or improve work performance or conduct.
- Reference to any relevant rule, regulation, or policy.
- Whether the disciplinary penalty is demotion, suspension without pay, or dismissal.
- The effective date if demotion or dismissal is imposed.

The specific period for a suspension without pay if applicable, not to exceed five working days.

**Rationale/
Source**

This policy meets the requirements of the following:
Health Insurance Portability and Accountability Act (HIPAA) Privacy Regulations
Section 45 CFR 164.503(e)(1)

**Cross
References**

For additional information, refer to the following:

Document Name
Organizational Policies and Procedure for Privacy and Security Employee Confidentiality Agreement

**Review or
Revision Date**

This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance

Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Security Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

POLICY FOR TERMINATION OF EMPLOYEES

[Insert Logo or Organization Name]

Corporate Security Policy

Dates: **Latest Revision:** April 14, 2003

Replaces: **Original Effective Date:**

Purpose

The purpose of this policy is to provide guidance for management and workforce members regarding the termination of employees that have violated the policies and procedures of **[NAME OF ORGANIZATION]'s**.

Policy

All employees are expected to review and understand their job function, its performance requirements and all business practices, procedures, and standards of conduct established by **[NAME OF ORGANIZATION]**. Any employee that violates the written policies, procedures, standards of conduct or does not fulfill the duties of their job function may be subject to termination.

The Following Conduct May Result in Termination:

Work Performance

Failure of an employee to maintain satisfactory work performance standards. The term "work performance" includes all aspects of an employee's work.

When, in the opinion of the administrator or supervisor, the employee's work performance is below standard, the administrator or supervisor will notify the employee in writing. If the employee's work performance does not improve the employee may be terminated.

Misconduct

All employees are expected to maintain standards of conduct suitable and acceptable to the work environment. Employees will be notified in writing if their conduct is not suitable. Misconduct is defined further in the **Policy for Sanctioning and Disciplining Employees**.

Violation of Internal Policies

All employees are required to follow the privacy and security policies of **[NAME OF ORGANIZATION]**. Violations of the organization's policies and procedures may be grounds for termination.

Procedure

All incidents that may result in termination should be investigated by **[NAME OF ORGANIZATION]'s** Privacy or Security Officer. If the investigation results in evidence that establishes with reasonable certainty that the employee engaged in conduct which warrants termination specific examples of the incident, as well as any disciplinary action taken, should be documented and recorded in the employee’s file.

A designated official of **[NAME OF ORGANIZATION]** should conduct an exit interview where the employee is notified of termination and is provided with a written reason for the termination. The following items should be addressed during the exit interview:

Access to Facility and Resources

If the employee has a key, badge, or any access device to the facility it should be turned over to the designated official during the exit interview. If the employee has access to the alarm system the code should be changed. The employee should turnover any purchasing cards, telephone cards, or company resources. If the employee has purchasing power the suppliers and vendors should be contacted to cancel employee as an authorized purchaser.

Personnel

The employee's name should be removed from the company directory and any company listings. If the employee is currently receiving medical, dental or 401k benefits from **[NAME OF ORGANIZATION]** the employee should be notified as to when the benefits will no longer be provided.

Payroll

If applicable, the employee's final time sheet should be submitted and final pay disposition should be discussed.

Access to Electronic Systems

If feasible the employee's access to **[NAME OF ORGANIZATION]'s** information systems should be removed as the exit interview is taking place. If necessary the employee's E-mail account should be forwarded to the Security Officer or appropriate individual. Voicemail access should be eliminated and the employee should turnover any electronic devices that are property of **[NAME OF ORGANIZATION]**.

**Rationale/
Source**

This policy meets the requirements of the following:
Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security

**Cross
References**

For additional information, refer to the following:

Document Name
Policy for Sanctioning and Disciplining Employees
Policy for Violations of Internal Policies

**Review or
Revision Date**

This policy is reviewed and approved annually, and as revised.

MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY	MM/DD/YYYY

Governance

Responsibility for adoption and/or implementation of this policy is as follows:

Approving Body		Executive Approval	
Security Officer/Management	00/00/03	Signature on File	00/00/03
	Date	Principal of Organization	Date

WORKFORCE STATEMENT OF UNDERSTANDING

I, _____, acknowledge that I have received training on the Health Insurance Portability and Accountability Act (HIPAA) and the business practices in affect at **[NAME OF ORGANIZATION]**.

I have reviewed, understand, and agree to abide by the following privacy and security practices:

- General Privacy
- Patient Privacy Rights
- Uses and Disclosures of Protected Health Information
- Minimum Necessary Information
- Administrative, Technical and Physical Safeguards
- Uses and Disclosures for Marketing
- Business Associate Relationships
- Enforcement, Sanctions, and Penalties for Violations of Individual Privacy

I understand that I am responsible for ensuring the security, integrity and confidentiality of patient health information created, obtained and/or maintained by **[NAME OF ORGANIZATION]**.

I understand that non-compliance will be cause for disciplinary action up to and including dismissal from **[NAME OF ORGANIZATION]**, and possible legal actions for violations of applicable regulations and laws.

I agree to promptly report all violations or suspected violations of any of the above policies to **[NAME OF ORGANIZATION]'s** Privacy Officer.

DATE: _____/_____/_____

Name of Employee

Employee's Signature

Social Security Number

Street Address

City

ST

Zip