

ExpressHEALTH Clinic Corporation
HIPAA Privacy Table of Contents

PREFACE ---page 2

1. GENERAL RULES

Designated Record Set ---page 3

Minimum Necessary Uses and Disclosures of Protected Health Information -- page 5

Notice of Privacy Practices ---page 10

Safeguarding and Storing Protected Health Information ---page 14

Emailing Protected Health Information ---page 18

Faxing Protected Health Information ---page 19

2. USES AND DISCLOSURES

Uses and Disclosures of Protected Health Information ---page 21

Authorization for Release of Protected Health Information ---page 27 (*Forms on page 30 & 31)

Uses and Disclosures of Protected Health Information for Research --- page 32

3. RIGHTS OF PATIENTS

Former Patients' Access to Protected Health Information ---page 34

Current Patients' Access to Protected Health Information ---page 43

Accounting of Disclosures of Protected Health Information ---page 45

Amendment of Protected Health Information ---page 52

Alternate Communications of Protected Health Information Complaints ---page 64

Restrictions to Permitted Uses and Disclosures of Protected Health Information ---page 73

4. OTHER REQUIREMENTS

Business Associates ---page 78

De-Identification of Protected Health Information ---page 84

Marketing and Fundraising ---page 86

Responding to a Subpoena ---page 88

Sanctions ---page 92

Verification of Identity and Authority of Officials Requesting PHI ---page 93

5. HIPAA DOCUMENTATION

Retention of Protected Health Information ----page 95

Destruction of Protected Health Information ---page 96

6. GLOSSARY ---page 100

PREFACE

Health facilities have a long-standing commitment to protecting the privacy of patient health information which is sometimes referred to as Protected Health Information (“PHI”). A part of this commitment involves compliance with the privacy standards contained in the regulations promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the first comprehensive federal protection of health information. The regulation is known as the Privacy Rule.

The following is a general overview of the requirements of the HIPAA privacy regulations. Each facility is referred to as a “Covered Entity” by these regulations and in this statement.

The HIPAA regulations govern the use and disclosure of PHI. In general, a Covered Entity may use PHI for purposes of treatment, payment, and health care operations. It may disclose PHI

1. With the individual’s authorization;
2. To another healthcare provider for treatment and payment purposes with the individual’s authorization; and
3. In certain other circumstances described by the regulations.

In using or disclosing PHI a Covered Entity must restrict the use or disclosure to the minimum amount necessary to accomplish the purpose of the use or disclosure. Employees of a Covered Entity will be assigned classifications that will determine the employees’ access to PHI in order to comply with the minimum necessary requirement.

The HIPAA regulations also give individuals several rights with respect to their PHI. In addition to the rights to have access and to receive confidential communications about PHI, the individual may copy and inspect PHI, restrict its use and disclosure, amend it, and receive an accounting of disclosures made of their PHI.

There are many obligations imposed on a Covered Entity by the privacy regulations. These

- Include developing and implementing policies and procedures to assure compliance;
- Training members of its workforce in the HIPAA requirements appropriate to their jobs;
- Documenting its efforts to achieve compliance; developing and implementing safeguards to protect PHI; and
- Designating a Privacy Officer.

A Privacy Officer is an individual designated by the Covered Entity who is responsible for the development and implementation of the required policies and procedures for compliance with HIPAA. The Covered Entity must also designate a person, who may be the Privacy Officer, to handle

complaints and to provide information about the entity's practices with respect to PHI.

The Covered Entity must state its practices with respect to the use and disclosure of PHI, the individual's rights and the Covered Entity's obligations in a "Notice of Privacy Practices". This Notice must be given to individuals at the time the treatment relationship begins.

NOTE: Express Health Clinic Corporation will be referred to as the "Facility" throughout this policy manual.

Designated Record Set

Purpose

To describe the documents that comprise the Designated Record Set.

Policy

The HIPAA Privacy Rule requires that patients be permitted to request access and amendment to their Protected Health Information ("PHI") that is maintained in a Designated Record Set. This policy documents the contents of the Designated Record Set.

Procedure

1. The Designated Record Set is a group of records maintained by or for the Facility that consists of the Medical Records and billing records about a patient and is used, in whole or in part, by or for the Facility to make decisions about the patient. The term *record* means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for the Facility.
2. The Facility maintains the following as the Designated Record Set:
 - a. The patient's Medical Record,
 - b. The patient's Business Office File, and
 - c. The patient's Personal Health Records.
3. The Patient Medical Record includes, at a minimum, the following:
 - Medical documentation
 - Advance directives
 - Assessments, flow sheets
 - Care plan
 - Informed consent
 - History and physical exams and other related medical records
 - Minimum Data Set
 - Medication and treatment records
 - Nursing documentation/progress notes

- Physician and professional consultant notes
- Physician's orders
- Reports from lab, x-ray and other diagnostic tests
- Face sheet
- Social service documentation

a. Excluded from the Medical Record are source data, including photographs, films, monitoring strips, videotapes, slides, worksheets and daily communication sheets, and shadow files or charts, unless such data is used to make decisions related to the patient's care.

b. If records from other providers are used by the Facility to make decisions related to the care and treatment of the patient, then these records are considered part of the Designated Record Set as well as the Medical Record, e.g., history and physical, discharge summary and labs from previous acute care hospitalization.

4. The Patient's Business Office File includes, at a minimum, the following:

- Demographic documents
- Acknowledgment of receipt of the Facility's *Notice of Privacy Practices*
- Correspondence relating to coverage and payment from insurance companies, health plans, Medicare, Medicaid and other payor sources
- Patient's claim information, including claim, remittance, eligibility response, and claim status response
- Statements of account balance
- Collection activity documents and correspondence

5. Personal Health Records consist of the patient's personal health information provided to the Facility by the patient. If such records are used by the Facility to make health care related decisions, provide care services, or document observations, actions or instructions, then the records will be considered part of the Designated Record Set.

6. The following are excluded from the Designated Record Set: Administrative data, such as audit trails, appointment schedules and practice guidelines that do not imbed PHI. Also excluded are incident reports, quality assurance data, vital certificate worksheets, and derived data such as accreditation reports, anonymous patient data for research purposes, public health records and statistical reports.

7. The Designated Record Set is to be retained according to state and federal regulations and following Facility or company retention procedures.

MINIMUM NECESSARY USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

Purpose

To ensure the Facility's uses and disclosures of Protected Health Information ("PHI") are limited to the minimum necessary to accomplish the intended purpose.

Policy

It is the policy of the Facility to make a reasonable effort to use or disclose, or to request from another health care provider, the minimum amount of PHI required to achieve the particular use or disclosure unless an exception applies.

The Facility will identify people or classes of people in its work force who need access to PHI to carry out their duties, the category or categories of PHI to which access is needed, and any conditions appropriate to such access.

For any non-routine request for disclosure of PHI that does not meet an exception, the Facility will review the request for disclosure on an individual basis.

Minimum necessary requirements do not apply to disclosures to health care providers for treatment purposes.

Procedure

1. The Facility will identify role based access to PHI per job description, including:
 - a. People or classes of people in its workforce who need access to PHI to carry out their duties, and
 - b. The category or categories of PHI to which access is needed, including any conditions that may be relevant to such access.

(See Sample "Role Based Access to PHI" table following this Policy.)

2. The Facility, for any type of disclosure or request for disclosure that is made on a routine and recurring basis, will limit the disclosed PHI, or the request for disclosure, to that which is reasonably necessary to achieve the purpose of the disclosure or request. (See "Examples of Routine Requests and Disclosures" following this Policy.)

3. The Facility, for disclosures or requests for that are *not* made on a routine and recurring basis (non-routine disclosures), will review the request to verify that PHI disclosed or requested is the minimum necessary.

All requests for non-routine disclosures or requests that do not meet an exception will be reviewed using standard criteria.

4. Exceptions to minimum necessary requirements: The Facility will release information without concern for the minimum necessary standard as follows:
 - a. Disclosures to or requests by a health care provider for treatment.
 - b. Uses or disclosures made to the individual who is the subject of the PHI.

- c. Uses or disclosures made pursuant to an authorization signed by the individual.
 - d. Disclosures made to the Secretary of the U.S. Department of Health and Human Services (federal government).
 - e. Disclosures that are required by law (such as for Department of Health state surveys, federal surveys, public health reportable events, FDA as related to product quality, safety, effectiveness or recalls etc.).
 - f. Uses and disclosures that are required for compliance with the HIPAA Privacy Rule.
5. The Facility may use or disclose an individual’s entire Medical Record only when such use or disclosure is specifically justified as the amount that is reasonably necessary to accomplish the intended purpose or one of the exceptions noted above applies.
6. Requests for entire Medical Records that are not covered by an exception will be reviewed using standard criteria.
7. Reasonable Reliance: The Facility may rely on a requested disclosure as minimum necessary for the stated purpose(s) when:
- a. Making disclosures to public officials, if the official represents that the information is the minimum necessary for the stated purpose(s).
 - b. The information is requested by another covered entity (health care provider, clearinghouse or health plan).
 - c. The information is requested by a professional who is a member of the Facility’s workforce or is a Business Associate of the Facility for the purpose of providing professional services to the Facility, if the professional represents that the information requested is the minimum necessary for the stated purpose(s).
 - d. The information is requested for research purposes and the person requesting the information has provided documentation or representations to the Facility that meet the HIPAA Privacy Rule. Contact the Privacy Officer to assist in the determination of whether such requirements have been met. (See Policy “Uses and Disclosures of Protected Health Information for Research.”)
8. The Facility, upon determination that the use, disclosure or request for PHI is the minimum necessary or one of the above exceptions apply (see Items 4 and 6), will release the PHI to the requestor.
9. Facility Requests for PHI from Another Covered Entity: When requesting PHI from another Covered Entity, the Facility must limit its request for PHI to the amount reasonably necessary to accomplish the purpose for which the request is made. For requests that are made on a routine and recurring basis, the Facility shall take reasonable steps to insure that the request is limited to the amount of PHI reasonably necessary to accomplish the purpose for which the request is made.
- For requests that are not on a routine or recurring basis, the Facility shall evaluate the request according to the following criteria:
- a. Is the purpose for the request stated with specificity?
 - b. Is the amount of PHI to be disclosed limited to the intended purpose?
 - c. Have the requirements for supporting documentation, statements, or representations been satisfied? (See policy “Uses and Disclosures of Protected Health

Information” for specific requirements.)

- d. Have all applicable requirements of the HIPAA Privacy Rule been satisfied with respect to the request?

Express Health Clinic Corporation

ROLE BASED ACCESS TO Protected Health Information (PHI)

LEVEL 1: None – No Access to Designated Record Set (i.e. Volunteer)

LEVEL 2: May access minimum necessary PHI (not Designated Record Set) to complete assigned tasks and/or to document actions (i.e. PHI discussed)

LEVEL 3: Full access to the Medical Record subset of the Designated Record Set

LEVEL 4: Full access to the Business Office File subset of the Designated Record Set

Position	Access Level				Explanation/Duties Performed Requiring Access
	1	2	3	4	
Office Aide		x			Filing and organization of records
Human Resources	x				No access necessary
Administrator		x	x	x	Operations/Payment
Patient Care Coordinator Staff		x	x	x	Operations/Payment
Nurse Practitioner Clinical Staff		x	x	x	Treatment/Payment/Operations
Financial Staff		x		x	Operations/Payment
Management Staff		x	x	x	Treatment/Payment/Operations
Assistant Administrator		x	x	x	Operations/Payment
Business Office Manager		x	x	x	Operations/Payment
Business Office Staff		x		x	Operations/Payment
Certified Patient Care Technician		x	x	x	Treatment/Payment/Operations

Maintenance/Cleaning Staff	x				No access to PHI necessary
MDS Coordinator		x	x	x	Treatment/Payment/Operations
Medical Records Supervisor		x	x	x	Operations/Payment
Privacy Official		x	x	x	Treatment/Payment/Operations
Volunteers	x				

EXAMPLES OF ROUTINE REQUESTS AND DISCLOSURES:

Requester	Purpose	Disclosures
Ambulance Co.	Obtain demographic and insurance information for billing	Face sheet with patient demographics, diagnoses and insurance information
Collection Agency	Obtain payment on past due accounts	File of patient names, addresses, dates of service and amount owed.
Coroner	Investigate a suspicious death	Specific information requested
Disability Determination	Evaluate individual's medical condition in support of disability benefits	Specific information requested
Insurance Co	Substantiate care provided for payment	Specific information requested in claims attachment request
Life Insurance	Evaluate individual's medical condition for issuance of a life insurance policy	Discharge summaries for specified period of time
Public Official	Investigate accidents or crimes	Specific information requested
Healthcare oversight agency	Investigate a complaint	Protected health information related to complaint
General Public	Locate patient (if asked for by name)	Directory information only: patient name, room number

Pharmacy	Obtain demographic and insurance information for billing	Face sheet with patient demographics, diagnoses and insurance information
Physician or other practitioner	Obtain demographic and insurance information for billing	Face sheet with patient demographics, diagnoses and insurance information
State data commission	Support a statewide registry	File of specific data elements requested
Law enforcement	To locate a fugitive, missing person, material witness or suspect of a crime	Per response to criteria and review committee decisions: <i>may include:</i> <ul style="list-style-type: none"> • Name and address • Date and place of birth • Social security # • ABO blood type • Type of injury • Date and time of treatment • Date and time of death • Description of physical characteristics <p>**DO NOT DISCLOSE ANY DNA analysis, dental records or typing, sample of analysis of body fluids**</p>
Organ/tissue donations	Qualify donation use (academic, transplant, etc.)	Per response to criteria and review committee decision

NOTICE OF PRIVACY PRACTICES

PURPOSE

To ensure that a *Notice of Privacy Practices* is provided to, and acknowledged by, each patient or his/her personal representative upon admission to the Facility.

Policy

The Facility's policy is to provide a *Notice of Privacy Practices* ("Notice") to each patient upon each admission to the Facility, and make a good faith effort to obtain a signed *Acknowledgment of Receipt of Notice of Privacy Practices* ("Acknowledgment") from the patient.

(See sample *Notice* and *Acknowledgment* forms following this Policy.)

The *Notice* shall include all elements and statements that are required by law. The *Notice* shall inform the patient of:

- Uses and disclosures of Protected Health Information ("PHI") that may be made by the Facility;
- The patient's rights with respect to his PHI; and
- The Facility's legal duties with respect to such PHI.

Procedure

1. The *Notice* and Acknowledgment will be included in the standard Admission paperwork.
2. The Facility Staff will provide the *Notice* to the patient at the time of admission.
Note: In the case of an emergency treatment situation, the Facility will provide the *Notice* to the patient as soon as reasonably practicable after the emergency treatment situation.
3. The Admission Staff will make a good faith effort to obtain the patient's signature on the *Acknowledgment* at the time the *Notice* is provided. The *Notice* and signed *Acknowledgment* will be kept in the patient's electronic document file and Business Office File.
4. If the patient refuses or is otherwise unable to sign the *Acknowledgment*, the Staff will document, on the Acknowledgment form, what actions were taken to obtain the patient's signature on the *Acknowledgment* and the reason(s) why a signed *Acknowledgment* was not obtained. This document will then be placed in the patient's Business Office File.
5. The Facility will provide a copy of the written *Notice* to patients and to other persons upon request.
6. The Facility will post a copy of the *Notice* in a clear and prominent location such as the entrance lobby or similar location.
7. A current version of the *Notice* will be maintained on the Facility's website.
8. Whenever the *Notice* is revised, the Facility Privacy Official will assure that:
 - a. The revised *Notice* is made available upon request on or after the effective date of the revision; and
 - b. The revised *Notice* is posted in a clear and prominent location.
9. Material changes shall not be implemented prior to the effective date of the revised *Notice*.

10. A copy of each *Notice* issued by the Facility will be maintained for at least six years from the date it was last in effect.

11. Any member of the workforce who has knowledge of a violation or potential violation of this Policy must make a report directly to the Privacy Official. (See the Policy “Sanctions.”)

ExpressHEALTH Clinic Corporation

Notice of Privacy Practices

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

Effective January 1, 2007; revised January 1, 2011

During your treatment at ExpressHEALTH Clinic, our caregivers may gather information about your medical history and current health. This Notice of Privacy Practices explains how that information may be used and shared with others. It also explains your privacy rights regarding this information. ExpressHEALTH Clinic is required by law to abide by the terms of this Notice, to make sure that information that identifies you is kept private, and to give you this Notice of our legal duties and practices with respect to medical information about you.

Uses and Disclosures of your Health Information

1. ExpressHEALTH Clinic may use health information to carry out treatment, payment and health care operations. • Treatment is the provision, coordination or management of health care. For example, we may use and disclose your information to consult with a third party or to refer you to other health care providers. We have the right to use and disclose health information to pay for your health care and operate our business, and for your treatment by your health care providers. For example, we may use your health information: To provide health care treatment to you. We may use and disclose health information about you to provide, coordinate or manage your health care and related services. For example, we may use and disclose health information about you when you need a prescription, lab work, an x-ray, or other health care services. In addition, we may use and disclose health information about you when referring you to another health care provider. • Payment includes the activities necessary to obtain reimbursement for the provision of health care. For example, we may need to give your health plan information about treatment you received at ExpressHEALTH Clinic so your health plan will pay us or reimburse you for the treatment.

• Health care operations include the activities necessary for ExpressHEALTH Clinic to run its business operations. For example, we may use your information to review treatment and services and to evaluate the performance of our staff.

2. We may use or disclose your health information: • When required by federal, state, or local law.

• To support public health activities by reporting as required or authorized by state or federal law. These reports may include the reporting of exposure to a communicable disease or risk of spreading a disease or condition. • To cooperate with law enforcement officials for certain law enforcement purposes as directed by a court order, warrant, criminal subpoena, or other lawful process. • To report abuse or neglect • To support health oversight activities that are authorized by law, such as administrative or criminal investigations, inspections, licensure or disciplinary actions and other similar activities necessary for appropriate oversight of government benefit programs or functions. • When required by a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death or other duties as required by law. • When necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public and the disclosure is to a person reasonably able to prevent or lessen the threat, as consistent with applicable law and standards. • For judicial or administrative proceedings, when consistent with applicable law; in response to a valid court order, administrative order, a grand jury subpoena, or with your written consent. • For research purposes with your written authorization or as permitted by state law. • If you are a member of the armed forces, when requested by military command authorities. In this case ExpressHEALTH Clinic will release only the minimum of necessary information to the military commanding officer. • To business associates to perform functions on ExpressHEALTH Clinic's behalf, if the business associate has signed an agreement to protect

the confidentiality of the information.

3. Unless you object, we may disclose your health information to a family member, other relatives, or a close friend or any other person you identify if the information relates to that person's involvement in your health care. If you are unable to agree or object to the use or disclosure, we may disclose such information as necessary if we determine that it is in your best interest.

4. In other situations, your written authorization will be obtained before ExpressHEALTH Clinic will use or disclose your health information to third parties outside ExpressHEALTH Clinic. You have the right to revoke previously given written authorization, you must submit this request in writing to ExpressHEALTH Clinic Corporation privacy office, the address is listed below.

5. State and federal laws may be more stringent and may prohibit certain uses and disclosures identified above. When another law is more stringent than the Health Insurance Portability and Accountability Act (HIPAA), we will follow the more stringent requirements.

Patient Rights

1. You may request ExpressHEALTH Clinic to restrict uses and disclosures of your health information. However, ExpressHEALTH Clinic is not required to agree to the requested restriction. These requests should be made to ExpressHEALTH Clinic, Privacy Officer. Requests must be made in writing. In your request, you must tell us (a) what information you want to limit; (b) whether you want to limit ExpressHEALTH Clinic's use, disclosure, or both, and (c) to whom you want the limits to apply, for example, if you want to prohibit disclosures to your spouse.

2. You have the right to request confidential communications by alternative means or at alternative locations. For example, you may request that we communicate with you only by mail. We will accommodate all reasonable requests, but your request must specify how or where you wish to be contacted, and we may require you to provide information about how payment will be handled. You must request confidential communications in writing.

3. You have a right to inspect and obtain a copy of your health information that is used to make decisions about your care for as long as ExpressHEALTH Clinic maintains the information. This right does not apply to certain health information, including information compiled in reasonable anticipation of or for litigation and other information not subject to the right to access information under HIPAA. Requests for access to health information should be made in writing to ExpressHEALTH Clinic, Privacy Officer. If access is denied, you will be provided with a written explanation that sets forth the basis for the denial, a description of how you may review those rights and a description of how you may complain.

4. You have the right to request that ExpressHEALTH Clinic amend your health information if it is incorrect or incomplete. Requests for amendment of information should be made in writing to ExpressHEALTH Clinic, Privacy Officer, and you must provide a reason that supports your request to have the information changed. ExpressHEALTH Clinic may deny your request for an amendment if the request is not in writing and submitted to the Privacy Officer. In addition, we may deny your request A you ask us to amend information that (a) was not created by ExpressHEALTH Clinic (unless the person or entity that created the information is no longer available to make the amendment); (b) is not part of the medical information kept by ExpressHEALTH Clinic; (c) is not part of the information you would be permitted to inspect and copy; or (d) is accurate and complete.

5. At your request, ExpressHEALTH Clinic will provide you with an accounting of disclosures by ExpressHEALTH Clinic of your health information during the six years prior to the date of your request. However, such accounting will not include disclosures made: 1) to carry out treatment, payment or health care operations; 2) directly to you or your personal representatives; 3) prior to the effective date of this notice; or 4) based on your written authorization. If you request more than one accounting within a 12-month period, ExpressHEALTH Clinic will charge a reasonable, cost-based fee for each subsequent accounting. Requests for a request of an accounting of disclosures should be made in writing to ExpressHEALTH Clinic, Privacy Officer.

6. To obtain a paper copy of this notice, contact ExpressHEALTH Clinic, Privacy Officer.

7. You may exercise your rights through a personal representative as permitted or required by applicable law. Your

personal representative may be required to produce evidence of authority to act on your behalf before that person will be given access to your information or allowed to take any action for you.

8. If you believe your privacy rights have been violated you may complain to the ExpressHEALTH Clinic, Privacy Officer. You may also file a complaint with the Secretary of the U.S. Department of Health and Human Services. ExpressHEALTH Clinic will not retaliate against you for filing a complaint.

ExpressHEALTH Clinic Duties

This Notice is effective beginning January 1, 2007; revision made January 1, 2011. However, ExpressHEALTH Clinic reserves the right to change its privacy practices and this Notice, and to apply the changes to any health information received or maintained by ExpressHEALTH Clinic prior to the date of the changes. If the terms of this Notice are changed, a revised version will be available upon request and will be posted in a clear and prominent location. You may access the notice by visiting our website at: www.expresshealthclinic.com

Complaints, Questions, and Requests

You may direct your questions about this Notice or ExpressHEALTH Clinic's privacy practices, requests regarding your information, or other privacy or confidentiality concerns to: ExpressHEALTH Clinic Corporation

Attn: Privacy Officer

PO Box 385

Dandridge, TN 37725

Phone: 1-865-475-9969 x 102

SAFEGUARDING AND STORING PROTECTED HEALTH INFORMATION

Purpose

The purpose of this policy is to provide guidelines for the safeguarding of Protected Health Information (“PHI”) in the Facility and to limit unauthorized disclosures of PHI that is contained in a patient’s Medical Record, while at the same time ensuring that such PHI is easily accessible to those involved in the treatment of the patient.

Policy

The policy of this Facility is to ensure, to the extent possible, that PHI is not intentionally or unintentionally used or disclosed in a manner that would violate the HIPAA Privacy Rule or any other federal or state regulation governing confidentiality and privacy of health information. The following procedure is designed to prevent improper uses and disclosures of PHI and limit incidental uses and disclosures of PHI that is, or will be, contained in a patient’s Medical Record. At the same time, the Facility recognizes that easy access to all or part of a patient’s Medical Record by health care practitioners involved in a patient’s care (nurses, attending and consulting physicians, and others) is essential to ensure the efficient quality delivery of health care.

The Administrator is responsible for the security of all Medical Records. All staff members are responsible for the security of the active Medical Records at the clinic sites.

Procedure

The Facility Privacy Official and Administrator shall periodically monitor the Facility’s compliance regarding its reasonable efforts to safeguard PHI.

Safeguards for Verbal Uses

These procedures shall be followed, if reasonable by the Facility, for any meeting or conversation where PHI is discussed.

Meetings during which PHI is discussed:

1. Specific types of meetings where PHI may be discussed include, but are not limited to:
 - a. Reporting or sharing necessary patient information
 - b. Department Head meetings
 - c. Interdisciplinary Plan of Care meeting
 - d. Medicare meeting
 - e. Bill review meetings
2. Meetings will be conducted in an area that is not easily accessible to unauthorized persons.
3. Meetings will be conducted in a room with a door that closes, if possible.
4. Voices will be kept to a moderate level to avoid unauthorized persons from overhearing.

5. Only staff members who have a “need to know” the information will be present at the meeting. (See the Policy “Minimum Necessary Uses and Disclosures.”)
6. The PHI that is shared or discussed at the meeting will be limited to the minimum amount necessary to accomplish the purpose of sharing the PHI.

Telephone conversations:

1. Telephones used for discussing PHI are located in as private an area as possible.
2. Staff members will take reasonable measures to assure that unauthorized persons do not overhear telephone conversations involving PHI. Reasonable measures may include:
 - a. Lowering the voice
 - b. Requesting that unauthorized persons step away from the telephone area
 - c. Moving to a telephone in a more private area before continuing the conversation
3. PHI shared over the phone will be limited to the minimum amount necessary to accomplish the purpose of the use or disclosure.

In-Person conversations:

- In patient exam rooms
- With patient/family in public areas
- With authorized staff in public areas

Reasonable measures will be taken to assure that unauthorized persons do not overhear conversations involving PHI. Such measures may include:

1. Lowering the voice
2. Moving to a private area within the Facility
3. If in patient exam room, keep door shut

Safeguards for Written PHI

All documents containing PHI should be stored appropriately to reduce the potential for incidental use or disclosure. Documents should not be easily accessible to any unauthorized staff or visitors.

Active Records in Clinic Locations:

1. Active Medical Records shall be stored in an area that allows staff providing care to patients to access the records quickly and easily as needed.
2. Authorized staff shall review the Medical Record in the clinic only.
3. Active Medical Records shall not be left unattended or computer screens left on with PHI visible in the clinic where patients, visitors and unauthorized individuals could easily view the records.
4. Vaccination Administration Records, Treatment Administration Records, and other documents containing PHI shall not be left open and/or unattended.
5. Only authorized staff shall review the Medical Records. All authorized staff reviewing Medical Records shall do so in accordance with the minimum necessary standards.
6. Medical Records shall be protected from loss, damage and destruction.

Active Business Office Files:

Active Business Office Files shall be stored in a secure area that allows authorized staff access as needed.

Thinned Records, Inactive Medical Records:

1. Inactive Medical Records will be filed in a systematic manner in a location that ensures the privacy and security of the information. The Health Information Manager or a designee shall monitor storage and security of such Medical Records. When records are left unattended, records will be in a locked room, file cabinet or drawer.
2. The Administrator will identify and document those staff members with keys to stored Medical Records. The minimum number of staff necessary to assure that records are secure yet accessible shall have keys allowing access to stored Medical Records. Staff members with keys shall assure that the keys are not accessible to unauthorized individuals.
3. Inactive Medical Records must be signed out if removed from their designated storage area. Only authorized persons shall be allowed to sign out such records.
4. Records must be returned to storage promptly.
5. In the event that the confidentiality or security of PHI stored in an active or inactive Medical Record has been breached, the Facility Privacy Official and Administrator shall be notified immediately.
6. Facility procedure will be followed if Medical Records are missing.
7. In the event of a change in ownership of the Facility, the Medical Records shall be maintained as specified in the Purchase and Sale Agreement.

Inactive Business Office Files:

Inactive Business Office Files shall be stored in a systematic manner in a location that ensures privacy and security of the information.

PHI Not a Part of the Designated Record Set:

1. Use of "shadow" charts or files is discouraged.
2. Any documentation of PHI shall be stored in a location that ensures, to the extent possible, that such PHI is accessible only to authorized individuals.

Office Equipment Safeguards

Computer access:

1. Only staff members who need to use computers to accomplish work-related tasks shall have access to computer workstations or terminals.
2. All users of computer equipment must have unique login and passwords.
3. Passwords shall be changed every 90 days.
4. Posting, sharing and any other disclosure of passwords and/or access codes is **strongly discouraged**.
5. Access to computer-based PHI shall be limited to staff members who need the information for treatment, payment or health care operations.
6. Facility staff members shall log off their workstation when leaving the work area.

7. Computer monitors shall be positioned so that unauthorized persons cannot easily view information on the screen.
8. Employee access privileges will be removed promptly following their departure from employment.
9. Employees will immediately report any violations of this Policy to their supervisor, Administrator or Facility Privacy Official.

Printers, copiers and fax machines:

1. Printers will be located in areas not easily accessible to unauthorized persons.
2. If equipment cannot be relocated to a secure location, a sign will be posted near the equipment indicating that unauthorized persons are prohibited from viewing documents from the equipment. Sample language: "Only authorized staff may view documents generated by this (indicate printer, copier, fax, etc). Access to such documents by unauthorized persons is prohibited by federal law."
3. Documents containing PHI will be promptly removed from the printer, copier or fax machine and placed in an appropriate and secure location.
4. Documents containing PHI that must be disposed of due to error in printing will be destroyed by shredding or by placing the document in a secure recycling or shredding bin until destroyed.

Destruction

Written:

Documentation that is not part of the Medical Record and will not become part of the Medical Record (e.g., report sheets, files, notes, lists of vital signs, weights, etc.) shall be destroyed promptly when it is no longer needed by shredding or placing the information in a secure recycling or shredding bin until the time that it is destroyed.

Electronic:

Prior to the disposal of any computer equipment, including donation, sale or destruction, the Facility must determine if PHI has been stored in this equipment and will delete all PHI prior to the disposal of the equipment.

(See the Policy "Destruction of Protected Health Information" for additional guidelines.)

EMAILING PROTECTED HEALTH INFORMATION

Purpose

To ensure the appropriate use of the email system when transmitting Protected Health Information (“PHI”).

Policy

It is the policy of this Facility to protect the electronic transmission of PHI as well as to fulfill our duty to protect the confidentiality and integrity of patient PHI as required by law, professional ethics and accreditation requirements. The information released will be limited to the minimum necessary to meet the requestor’s needs. Whenever possible, de-identified information will be used.

Procedure

1. E-mail users will be set up with a unique identity complete with unique password and file access controls.
2. E-mail users may not intercept, disclose or assist in intercepting and disclosing e-mail communications.
3. Patient specific information regarding highly sensitive health information must not be sent via e-mail, even within the internal email system (i.e. information relating to AIDS/HIV, drug and alcohol abuse and psychotherapy notes).
4. Users will restrict their use of email for communicating normal business information such as information about general care and treatment of patients, operational and administrative matters, such as billing.
5. Users should verify the accuracy of the email address before sending any PHI and, if possible, use email addresses loaded in the system address book.
6. PHI may be sent unprotected via e-mail within a properly secured, internal network of the organization. When sending PHI outside of this network, such as over the Internet, every effort should be made to secure the confidentiality and privacy of the information. Sample security measures include password protecting the document(s) being sent or encrypting the message.
7. All e-mail containing PHI will contain a confidentiality statement.
8. Users should exercise extreme caution when forwarding messages. Sensitive information, including patient information, must not be forwarded to any party outside the organization without using the same security safeguards as specified above.
9. Users should periodically purge e-mail messages that are no longer needed for business purposes, per the organization’s records retention policy.
10. Employee e-mail access privileges will be removed promptly following their departure from the organization.
11. Email messages, regardless of content, should not be considered secure and private. The amount of information in any email will be limited to the minimum necessary to meet the needs of the recipient.
12. Employees should immediately report any violations of this guideline to their supervisor, Administrator or Facility Privacy Official.

FAXING PROTECTED HEALTH INFORMATION

Purpose

To ensure that Protected Health Information (“PHI”) is appropriately safeguarded when it is sent or received via facsimile (fax) machine or software.

Policy

It is the policy of this Facility to allow the use of facsimile machines to transmit and receive PHI. The information released will be limited to the minimum necessary to meet the requestor’s needs.

Procedure

1. The fax machine should be located in an area that is not easily accessible to unauthorized persons. Examples include the business office, medical record office or nurse’s station. If possible, the fax machine should not be located in a public area where confidentiality of PHI might be compromised. If this is not possible, a sign should be posted regarding access to the documents.
2. Received documents will be removed promptly from the fax machine. To promote secure delivery, instructions on the cover page will be followed.
3. Unless otherwise prohibited by state law, information transmitted via facsimile is acceptable and may be included in the patient’s Medical Record.
4. Steps should be taken to ensure that the fax transmission is sent to the appropriate destination. These include:
 - a. Pre-programming and testing destination numbers whenever possible to eliminate errors in transmission due to mis-dialing.
 - b. Asking frequent recipients to notify the Facility of a fax number change.
 - c. Confirming the accuracy of the recipient’s fax number before pressing the send/start key.
 - d. If possible, printing a confirmation of each fax transmission.
5. A cover page should be attached to any facsimile document that includes PHI. (See a sample cover page following this Policy.) The cover page should include:
 - a. Destination of the fax, including name, fax number and phone number;
 - b. Name, fax number and phone number of the sender;
 - c. Date;
 - d. Number of pages transmitted; and
 - e. Confidentiality Statement.
6. If a fax transmission fails to reach a recipient or if the sender becomes aware that a fax was misdirected, the internal logging system should be checked to obtain incorrect recipient’s fax number. Fax a letter to the receiver and ask that the material be returned or destroyed.
7. A written *Authorization* for any use or disclosure of PHI will be obtained when the use or

disclosure is not for treatment, payment or healthcare operations or required by federal or state law or regulation.

8. The PHI disclosed will be the minimum necessary to meet the requestor's needs.
9. Highly sensitive health information should not be sent by fax in certain states (e.g., information relating to AIDS/HIV, drug and alcohol abuse and psychotherapy notes).

Sample Confidentiality Statements:

The documents accompanying this transmission contain confidential protected health information that is legally privileged. This information is intended only for the use of the individual or entity named above. The authorized recipient of this information is prohibited from disclosing this information to any other party unless required to do so by law or regulation and is required to destroy the information after its stated need has been fulfilled.

If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this information in error, please notify the sender immediately and arrange for the return or destruction of these documents.

USES AND DISCLOSURES OF PROTECT HEALTH INFORMATION

Purpose

To ensure that disclosure of Protected Health Information (“PHI”) is made consistent with applicable laws, regulations and health information standards, and to ensure that any disclosures of a patient’s PHI to a patient’s family members, other relatives, close friends or other persons designated by the patient are appropriate.

Policy

Disclosure of PHI will only be allowed with a properly completed and signed authorization except:

- When required or allowed by law (see “Request and Disclosure Table” following this Policy).
- As defined in the *Notice of Privacy Practices*:
 - For continuing care (treatment)
 - To obtain payment for services (payment)
 - For the day-to-day operations of the facility and the care given to the patients (health care operations)

Disclosure of PHI will be centralized through the Facility Privacy Official. In some instances, the Facility Privacy Official will need to track information that is disclosed. All disclosures designated as trackable on the “Request and Disclosure Table” must be approved by the Privacy Official to enable the Facility to provide an accounting of disclosures when requested.

Disclosure of PHI will be carried out in accordance with all applicable legal requirements and in accordance with Facility policy. Each Facility will be responsible for researching and abiding by applicable state laws and regulations.

Original Medical Records will not be removed from the premises, except when ordered by subpoena or by other court order.

Procedure

Receiving a Request for Medical Records:

Requests for Medical Records shall be managed by the Facility Privacy Official.

1. Other staff members will not release PHI without approval of the Facility Privacy Official.
2. Only emergency release of information will be done after hours or on weekends.
3. After hours and on weekends, release of information for continuing care (i.e., transfer to a hospital or emergency clinic) is allowed.

Responding to Specific Types of Disclosures:

See the “Request and Disclosure Table” following this Policy for applicable requirements in responding to requests by specific entities/individuals.

1. Media: No PHI shall be released to the news media or commercial organizations without

the authorization of the patient or his personal representative.

2. Telephone Requests: Staff members receiving requests for PHI via the telephone will make reasonable efforts to identify and verify that the requesting party is entitled to receive such information.

Disclosures to Persons Involved with a patient's Care:

1. The Facility may disclose to a family member, other relative, close friend, or any other person identified by the patient, PHI:

- a. That is directly relevant to that person's involvement with the patient's care or payment for care; or
- b. To notify such person of the patient's location, general condition, or death.

2. Conditions if the patient is Present. If the patient is present for, or otherwise available, prior to a permitted disclosure, then the Facility may use or disclose the PHI only if the Facility:

- a. Obtains the patient's agreement;
- b. Provides the patient with an opportunity to object to the disclosure, and the patient does not express an objection (this opportunity to object and the patient's response may be done orally); or
- c. May reasonably infer from the circumstances, based on the exercise of professional judgment, that the patient does not object to the disclosure.

3. Conditions if the patient is Not Present or is Incapacitated. The Facility may, in the exercise of professional judgment, determine whether the disclosure is in the best interest of the patient, and, if so, disclose only that PHI which is directly relevant to the person's involvement with the patient's care if:

- a. The patient is not present,
- b. The opportunity to agree/object to the use or disclosure cannot practicably be provided because of the patient's incapacity, or
- c. In an emergency.

4. Confirming Identity. The Facility shall take reasonable steps to confirm the identity of a patient's family member or friend. The Facility is permitted to rely on the circumstances as confirmation of involvement in care. For example, the fact that a person brings a patient to the Facility and is present during the office visit is sufficient confirmation of involvement in the patient's care.

REQUEST AND DISCLOSURE TABLE

<i>Requestor</i>	<i>Authorization Required?</i>	<i>Copy Fee Charged?</i>	<i>Track on Accounting of Disclosure?</i>	<i>Notes:</i>
Accrediting Agencies (JCAHO, CARF)	No	No	No	See policy on Business Associates
Attorney for patient	Yes	Yes	No	See policy on Authorizations
Attorney for Facility/Corporation	No	No	No	See policy on Business Associates
Contractors/ Business Associates	No, unless their purpose falls outside of TPO	No	No	See policy on Business Associates
For Deceased Persons <input type="checkbox"/> Coroner or Medical Examiner, Funeral Directors <input type="checkbox"/> Organ Procurement	No	No	Yes	See policy on Accounting of Disclosures
Employer <input type="checkbox"/> PHI specific to work related illness or injury, and <input type="checkbox"/> Required for employer's compliance with occupational safety and health laws	No, for the purpose listed. Yes for all others.	No	No	
Family Members	No for oral disclosures to family members involved in care; Yes for others	Yes	No	See policy on Authorizations

			<i>Track on Accounting of Disclosure?</i>	
<i>Requestor</i>	<i>Authorization Required?</i>	<i>Copy Fee Charged?</i>		<i>Notes:</i>
Entity Subject to the Food and Drug Administration	No	No	Yes	See policy on Accounting of Disclosures
<input type="checkbox"/> Adverse events, product defects or biological product deviations <input type="checkbox"/> Track products <input type="checkbox"/> Enable product recalls, repairs, or replacements <input type="checkbox"/> Conduct post marketing surveillance				
Health Oversight	No	No	Yes	See policy on Accounting of Disclosures
<input type="checkbox"/> Government benefits program <input type="checkbox"/> Fraud and abuse compliance <input type="checkbox"/> Civil rights laws <input type="checkbox"/> Trauma/tumor registries <input type="checkbox"/> Vital statistics <input type="checkbox"/> Reporting of abuse or neglect				
Health Care Practitioners and Providers for Continuity of Treatment and Payment	No	No	No	Part of treatment
Health Care Practitioners and Providers if <u>not</u> Involved in Care or Treatment (i.e., consultants)	No	No	No	Part of operations
Insurance Companies/Third Party Payors	No	No	No	Part of payment
Related to Claims Processing				
Judicial and Administrative Proceedings				See policy on Accounting of Disclosures

			<i>Track on Accounting of Disclosure?</i>	
<i>Requestor</i>	<i>Authorization Required?</i>	<i>Copy Fee Charged?</i>		<i>Notes:</i>
<input type="checkbox"/> Court order, or warrant	No	No	Yes	
<input type="checkbox"/> Subpoena	No - See policy on Responding to a Subpoena	Yes	Yes	
Law Enforcement	No	No	Yes, except for disclosures to correctional institutions.	See policy on Accounting of Disclosures
<input type="checkbox"/> Administrative request				
<input type="checkbox"/> Locating a suspect, fugitive, material witness or missing person				
<input type="checkbox"/> Victims of crime				
<input type="checkbox"/> Crimes on premises				
<input type="checkbox"/> Suspicious deaths				
<input type="checkbox"/> Avert a serious threat to health or safety				
Public Health Authorities	No	No	Yes	See policy on Accounting of Disclosures
<input type="checkbox"/> Surveillance				
<input type="checkbox"/> Investigations				
<input type="checkbox"/> Interventions				
<input type="checkbox"/> Foreign governments collaborating with US public health authorities				
<input type="checkbox"/> Recording births/deaths				
<input type="checkbox"/> Child/elder abuse				
<input type="checkbox"/> Prevent serious harm				
<input type="checkbox"/> Communicable disease				
Research (w/o Authorization)	No, if IRB or Privacy Board approves the	No	Yes	See policy on Uses and Disclosures for Research and policy

<i>Requestor</i>	<i>Authorization Required?</i>	<i>Copy Fee Charged?</i>	<i>Track on Accounting of Disclosure?</i>	<i>Notes:</i>
	research study and waives authorization.			on Accounting of Disclosures
patient/patient's Personal Representative	No	Yes	No	See policy on Authorizations
Specialized Government Functions	No	No	Yes, except for disclosures for national security and intelligence activities.	See policy on Accounting of Disclosures
<input type="checkbox"/> Military and Veterans' activities				
<input type="checkbox"/> Protective services for the Ppatient				
<input type="checkbox"/> Foreign military personnel				
<input type="checkbox"/> National security and intelligence activities				
Workers' Compensation	No	See applicable state law	Yes	See policy on Accounting of Disclosures
<input type="checkbox"/> Comply w/existing laws (see state law)				

This does not apply to PHI created or maintained prior to April 14, 2003.

AUTHORIZATION FOR RELEASE OF PROTECTED HEALTH INFORMATION

Purpose

The purpose of this Policy is to set forth the Facility's process for the use and disclosure of Protected Health Information ("PHI") pursuant to a written authorization.

Policy

In accordance with the HIPAA Privacy Rule, when PHI is to be used or disclosed for purposes other than treatment, payment, or health care operations, the Facility will use and disclose it only pursuant to a valid, written authorization, unless such use or disclosure is otherwise permitted or required by law. Use or disclosure pursuant to an authorization will be consistent with the terms of such authorization.

Procedure

Exceptions to Authorization Requirements

PHI may be disclosed without an authorization if the disclosure is:

1. Requested by the patient or his personal representative (authorization is never required);
2. For the purpose of treatment;
3. For the purpose of the Facility's payment activities, or the payment activities of the entity receiving the PHI;
4. For the purpose of the Facility's health care operations;
5. In limited circumstances, for the health care operations of another Covered Entity, if the other Covered Entity has or had a relationship with the patient;
6. To the Secretary of the U.S. Department of Health and Human Services for the purpose of determining compliance with the HIPAA Privacy Rule; or
7. Required by other state or federal law. (See "Request and Disclosure Table" in the "Uses and Disclosures of Protected Health Information" Policy for other exceptions.)

Use or Disclosure Pursuant to an Authorization

1. When the Facility receives a request for disclosure of PHI, the Facility Privacy Official shall determine whether an authorization is required prior to disclosing the PHI.
2. PHI may never be used or disclosed in the absence of a valid written authorization if the use or disclosure is:
 - a. Of psychotherapy notes as defined by the HIPAA Privacy Rule;
 - b. For the purpose of marketing; or
 - c. For the purpose of fundraising.
3. If the use or disclosure requires a written authorization, the Facility shall not use or disclose the PHI unless the request for disclosure is accompanied by a valid authorization.
4. If the request for disclosure is not accompanied by a written authorization, the Facility Privacy Official shall notify the requestor that it is unable to provide the PHI requested. The Privacy

Official will supply the requestor with an *Authorization to Use or Disclose PHI* ("*Authorization*") form. (See sample *Authorization* form following this Policy.)

5. If the request for disclosure is accompanied by a written authorization, the Privacy Official will review the authorization to assure that it is valid (see the "Checklist for Valid Authorization" following this Policy).
6. If the authorization is lacking a required element or does not otherwise satisfy the HIPAA requirements, the Privacy Official will notify the requestor, in writing, of the deficiencies in the authorization. No PHI will be disclosed unless and until a valid authorization is received.
7. If the authorization is valid, the Privacy Official will disclose the requested PHI to the requester. Only the PHI specified in the authorization will be disclosed.
8. Each authorization shall be filed in the patient's Medical Record.

Preparing an Authorization for Use or Disclosure

1. When the Facility is using or disclosing PHI and an authorization is required for the use or disclosure, the Facility will not use or disclose the PHI without a valid written authorization from the patient or the patient's personal representative.
2. The *Authorization* form must be fully completed, signed and dated by the patient or the patient's personal representative before the PHI is used or disclosed.
3. The Facility may not condition the provision of treatment on the receipt of an authorization except in the following limited circumstances:
 - a. The provision of research-related treatment; or
 - b. The provision of health care that is solely for the purpose of creating PHI for disclosure to a third party (i.e., performing an independent medical examination at the request of an insurer or other third party).
4. An authorization may not be combined with any other document unless one of the following exceptions applies:
 - a. Authorizations to use or disclose PHI for a research study may be combined with any other type of written permission for the same research study, including a consent to participate in such research;
 - b. Authorizations to use or disclose psychotherapy notes may only be combined with another authorization related to psychotherapy notes; or
 - c. Authorizations to use or disclose PHI other than psychotherapy notes may be combined, but only if the Facility has not conditioned the provision of treatment or payment upon obtaining the authorization.

Revocation of Authorization

1. The patient may revoke his authorization at any time.
2. The authorization may ONLY be revoked in writing. If the patient or the patient's personal representative informs the Facility that he/she wants to revoke the authorization, the Facility will assist him/her to revoke in writing.
3. Upon receipt of a written revocation, the Privacy Official will write the effective date of the revocation on the *Authorization* form.

4. Upon receipt of a written revocation, the Facility may no longer use or disclose a patient's PHI pursuant to the authorization.
5. Each revocation will be filed in the patient's Medical Record.

AUTHORIZATION TO DISCLOSE HEALTH INFORMATION

Individual who's Health Information is being authorized to be disclosed:

Named Individual: _____ Date of Birth _____

1. I am the Named Individual and I am at least eighteen (18) years old ();
if the named Individual is less than eighteen (18) years old, I am (a) the Parent and Natural Guardian () or (b) the Legal Guardian or Legal Custodian () of the Named Individual, and I am legally authorized to execute this document.
2. I hereby authorize the following Disclosing Entity to disclose the Health Information related to the Named Individual to the following :

Name of Disclosing Person or Entity: **Express Health Clinic Corporation**

3. I hereby authorize the Disclosing Person or Entity to disclose Health Information of the Named Individual as hereafter indicated to and for the use of:

Name of Person or Organization: _____

Attention: _____

Address: _____ ; Telephone: _____

Address: _____ ; Fax: _____

4. The Health Information authorized to be disclosed for the dates indicated, where applicable, is as follows (indicate dates where appropriate):

- () **Entire Record, or**
- () immunization record
- () history and physical
- () allergies
- () medication list
- () physical therapy progress and _____ evaluation notes
- () problem list
- () consultation record
- () office notes from (date) _____ to present
- () laboratory results from (date) _____ to present
- () Other: _____

5. I understand that authorizing the disclosure of this Health Information is voluntary and that the information in my health records may include information relating to sexually transmitted disease, acquired immunodeficiency syndrome (AIDS), human immunodeficiency virus (HIV), behavioral or mental health services and treatment for alcohol and drug abuse. I understand any disclosure of information carries with it the potential for an unauthorized re-disclosure and the information may not be protected by federal confidentiality rules.

6. I understand I have the right to revoke this authorization at any time by doing so in writing and presenting my written revocation to the Disclosing Person or Entity, but the revocation will not apply to (1) information that has already been released in response to this authorization, or (2) my health insurance company, if any. Unless otherwise revoked, this authorization will expire on the earlier of the following date if any is specified: _____ or six (6) months from the date of this Authorization.

Signature of Named Individual or applicable Parent, Guardian or Custodian:

_____ and Date Signed: _____

AUTHORIZATION TO DISCLOSE HEALTH INFORMATION

Individual who's Health Information is being authorized to be disclosed:

Named Individual: _____ Date of Birth _____

7. I am the Named Individual and I am at least eighteen (18) years old (); if the named Individual is less than eighteen (18) years old, I am (a) the Parent and Natural Guardian () or (b) the Legal Guardian or Legal Custodian () of the Named Individual, and I am legally authorized to execute this document.

8. I hereby authorize the following Disclosing Person or Entity to disclose the Health Information related to the Named Individual:

Name of Disclosing Person or Entity: _____

9. I hereby authorize the Disclosing Person or Entity to disclose Health Information of the Named Individual as hereafter indicated to and for the use of:

Express Health Clinic

Attention: _____

Address: _____ Telephone: _____

Address: _____ Fax: _____

10. The Health Information authorized to be disclosed for the dates indicated, where applicable, is as follows (indicate dates where appropriate):

- () **Entire Record, or**
- () immunization record
- () history and physical
- () allergies
- () medication list
- () physical therapy progress and evaluation notes
- () problem list
- () consultation record
- () office notes from (date) _____ to present
- () laboratory results from (date) _____ to present
- () Other: _____

11. I understand that authorizing the disclosure of this Health Information is voluntary and that the information in my health records may include information relating to sexually transmitted disease, acquired immunodeficiency syndrome (AIDS), human immunodeficiency virus (HIV), behavioral or mental health services and treatment for alcohol and drug abuse. I understand any disclosure of information carries with it the potential for an unauthorized re-disclosure and the information may not be protected by federal confidentiality rules.

12. I understand I have the right to revoke this authorization at any time by doing so in writing and presenting my written revocation to the Disclosing Person or Entity, but the revocation will not apply to (1) information that has already been released in response to this authorization, or (2) my health insurance company, if any. Unless otherwise revoked, this authorization will expire on the earlier of the following date if any is specified: _____ or six (6) months from the date of this Authorization.

Signature of Named Individual or applicable Parent, Guardian or Custodian:

_____ and Date Signed: _____

USES AND DISCLOSURE OF PROTECTED HEALTH INFORMATION FOR RESEARCH

Purpose

To provide guidance on the use and/or disclosure of Protected Health Information (“PHI”) for research purposes.

Policy

The Facility must obtain a patient's authorization before releasing his/her PHI for research purposes.

The Facility will ensure that an appropriately instituted and formally designated (per Federal Drug Administration/FDA regulations) Institutional Review Board is utilized for the protection of human subjects in any research activity involving access to PHI under the Facility’s control.

The patient has the right to refuse to participate in research. (See *F155* in the State Operations Manual.)

The Facility shall abide by the experimental subject’s (patient’s) privacy rights.

Procedure

1. Federal regulations and state laws regulate the use of human subjects (patients) in any investigation designed to develop or contribute to specific knowledge. Such laws require that specific information be disclosed so that a subject (patient) may give informed authorization and that authorization must be documented.
 - a. At the beginning of any research project, the Facility and the entity involved in the research must determine and agree on who will be responsible for obtaining an authorization to use or disclose PHI.
 - b. If an outside authorization is utilized, the Facility Privacy Designee will review the patient’s authorization to assure that it is valid in accordance with the HIPAA Privacy Rules and those special provisions related to research. (See Policy “Authorization for Release of Protected Health Information.”)
 - c. Special Authorization Provisions Related to Research
 - i. Expiration Date: The *Authorization* form will state the expiration date or that the expiration event is “end of research study,” “none,” or similar language.
 - ii. Combining Authorization: The *Authorization* form may be combined with any other type of written permission for the same research study, including another authorization for the use or disclosure of PHI for such research or a consent to participate in such research.
 - iii. Condition Treatment on Authorization: The provision of research-related treatment may be conditioned on the provision of an authorization for the use or disclosure of PHI for such research.

2. Federal law requires the establishment of an Institutional Review Board (“IRB”) to review and approve proposed research and the process by which the investigator intends to secure the informed authorization of participants.
 - a. Institutions engaged in research involving human subjects (e.g., medical schools, universities, large hospitals) will usually have their own IRB to oversee research conducted within the institution or by staff of the institution.
 - b. It is the responsibility of the organization or institution conducting the research to establish or contract with an IRB; it is the Facility’s responsibility to ensure that an IRB is utilized.
3. If the research study is approved by the IRB and de-identified health information can be used or disclosed, then no further privacy implications exist. (See the Policy “De-Identification of Protected Health Information” for details of how to de-identify the health information for disclosure.)
4. If the research study is approved by the IRB and de-identified health information cannot be used or disclosed, then an *Authorization* form is required and must be obtained from each patient included in the research study.
5. Appropriate Facility staff will manage requests to participate in research studies and coordinate the review process by the IRB.
 - a. Contact/communications with the IRB and related findings must be documented and communicated to the Facility Privacy Designee.
 - b. If the Facility participates in research projects, the Facility Privacy Designee must have a method of tracking the correspondence, decisions and other communications regarding the research project.
6. The Facility will inform every patient of any research or economic interest (for example, any direct or indirect remuneration that may come to the Facility as a result of the research) that may result from his or her treatment.
7. The Facility or the entity conducting the research will obtain the patient’s *Authorization* form when required. (See Item 1.)
8. The Facility Privacy Designee will file the original copy of the request and the associated response in the participant’s Medical Record.

RIGHTS OF PATIENTS SECTION: **PATIENT ACCESS TO PROTECTED HEALTH** **INFORMATION**

Purpose

To define former patients' right to access their Medical Records and explain requirements imposed by the Health Insurance Portability and Accountability Act (HIPAA) Final Privacy Rule. The Privacy Rule explains the rights of patients, including access to their Medical Records, and specifies required time frames for responding to patient requests for access.

Policy

Every patient has the right to access his or her Protected Health Information ("PHI"). The right of access is not absolute and there may be situations where access is not allowed; however, the Facility will respond to all requests to access a patient's health information. Some states may have more stringent regulations and it is the responsibility of each Facility to research state laws. The Privacy Rule specifies the time for responding to requests for access. These time lines must be adhered to unless state laws require the Facility to respond in a shorter time frame.

Note: OBRA requirements are more stringent than HIPAA Privacy Rule requirements. Therefore, the Facility must meet the OBRA time frames for current patients.

Procedure

1. A patient will be notified of the right to access PHI in the Facility's *Notice of Privacy Practices*. The *Notice of Privacy Practices* is given to the patient upon admission to the Facility.
2. A patient has the right to inspect and obtain a copy of PHI in his or her Designated Record Set, except for information compiled in reasonable anticipation of, or for use in a civil, criminal, or administrative action or proceeding.
3. Requests for access to PHI and release of information will be managed by the Facility Privacy Official or the Medical Record Coordinator/Health Information Manager.
4. The patient or representative will be provided with a copy of an *Access to Protected Health Information* ("Access") form upon receiving an inquiry from a patient to obtain copies of his or her PHI. The request will not be evaluated until the form is completed. (See sample *Access* form following this Policy.)
5. If a former patient or patient's personal representative requests to view or review PHI, the Facility must respond to the request within 30 days.
6. A reasonable cost-based fee may be charged for the copies provided. The cost per page may not exceed the state statute for copying costs. In the absence of a state statute, the fee will include the cost of the supplies and labor used in preparing the copy and postage, if applicable.
7. Processing the Request and Providing Access to the PHI:
 - a. The Facility must respond to a request from former patients within 30 days

of the receipt of the request if the PHI is available on-site. If the PHI is stored off-site, the Facility must take action within 60 days of the receipt of the request.

b. The Facility may have a one time extension of 30 days to the time frames noted in Item 7.a., provided that:

- i. A written statement of the reasons for the delay are provided, and
- ii. The date by which the Facility will complete its action on the request is stated.

(See sample *Notification of Time Extension* form following this Policy.)

c. The Facility Privacy Official shall provide the patient with permitted access to the PHI in the form or format requested. If the PHI is not accessible in the format requested, a readable hard copy or a format to which the Facility and the patient agree is acceptable will be provided.

d. The Facility may provide a summary of the PHI requested if the patient agrees, in advance, to this summary and to any fees imposed. (A summary is a recapitulation of the patient's Medical Record done by a physician or health care professional.)

8. Guidelines for Denying the Request for Access to PHI:

a. The Facility must provide a timely, written denial to the individual, which includes the basis for the denial, and, if applicable, a statement of the individual's review rights. In addition, it must provide a description of how the individual may complain to the Facility or to the Secretary of the Office of Civil Rights.

b. The Facility may deny the request if the PHI is not contained in its Designated Record Set.

c. The Facility may deny the request for access to a patient's PHI without a right to review if:

- i. The request is for information compiled in anticipation of a legal proceeding; or
- ii. The request is for PHI created or obtained during the course of research which includes treatment for as long as the research continues, provided that the patient has agreed to the denial of access and the Facility has informed the patient that this right will be reinstated upon completion of the research; or
- iii. The request is for PHI obtained from someone other than a provider under the promise of confidentiality and disclosure would likely reveal the source.

d. The Facility may deny the request for access to a patient's PHI provided that the patient has been given a right to review the denial if:

- i. A licensed health care professional has determined, in the exercise of professional judgment, that the access of requested PHI is reasonably likely to endanger the life or physical safety of the individual or another person; or
- ii. The PHI refers to another person (unless such other person is a health care provider (for example, a doctor) and a licensed health care professional has determined, in the exercise of professional judgment, that the

access requested is reasonably likely to cause substantial harm to such other person; or

iii. The individual's personal representative makes a request for access and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

9. Providing a Review Process for Denied Requests for Access to PHI:

patients have the right to request a review of the denial. If a request is received, the following steps must be taken:

- a. The Facility Privacy Official will promptly refer the request to review the denial to the Privacy Officer.
- b. The Privacy Officer shall refer the case to a licensed health professional who was not directly involved in the denial.
- c. The Facility shall promptly provide written notice of the results of the review and based on the review, take any necessary steps outlined in this Policy.

(See sample *Review Determination Letter* following this Policy.)

Express Health Clinic Corporation

ACCESS TO PROTECTED HEALTH INFORMATION

Date Received: _____

Initials of Privacy Official: _____

SECTION A: patient to complete the following information

Date: _____ Requestor Name: _____

Patient Name: _____ Medical Record Number _____

Patient Date of Birth _____

Address: _____

Facility Name: Express Health Clinic Corporation

REQUEST:

I hereby request that the Facility provide me with access to my Protected Health Information as checked below. **(Check all that apply):**

<input type="checkbox"/> The entire Medical Record (all information) to the above-named requestor	
<input type="checkbox"/> Activity documentation	<input type="checkbox"/> Medication and treatment records
<input type="checkbox"/> Admission/readmission documentation	<input type="checkbox"/> Office visit documentation/progress notes
<input type="checkbox"/> Advance directives	<input type="checkbox"/> Physician and professional consult progress notes
<input type="checkbox"/> Assessments, flow-sheets	<input type="checkbox"/> Reports from lab, x-ray, and other diagnostic tests
<input type="checkbox"/> Informed consent	<input type="checkbox"/> Face sheet
<input type="checkbox"/> History and physical exams and other related clinical records	
<input type="checkbox"/> Minimum Data Set	
<input type="checkbox"/> Other (Describe as specifically as possible:	

SECTION B: FOR FORMER PATIENTS ONLY
Facility to complete this section

Request for access or copy is Accepted Denied

If denied, check the reasons for denial:

PHI is not part of the patient’s Designated Record Set

Federal law forbids making the requested information available to the patient for inspection (e.g., CLIA or Privacy Act of 1974)

The requested information is psychotherapy notes

The requested information has been compiled for legal proceeding

The requested information was obtained under promise of confidentiality and access would be reasonably likely to reveal the source of the information

The requested information is temporarily unavailable because the individual is a research participant

Licensed health care provider has determined that access to the requested information would result in physical harm to the individual or others

Licensed health care provider has determined that the requested information identifies a third person who may be physically, emotionally, or psychologically harmed if access to the information is granted

Licensed health care provider has determined that access to the requested information by the patient’s personal representative could result in harm to the individual

We are acting under the direction of a correctional institution and letting the inmate access or obtain a copy of the requested information would jeopardize the health, safety, security, custody, or rehabilitation of another person at the correctional institution

The requested information is not maintained by our Facility

RIGHT TO REVIEW:

Yes

No – Contact the Facility Privacy Official with any questions.

You have a right to file a complaint with our Facility and may do so by contacting the Facility Privacy Official at: _____ (Facility phone number). You also have the right to file a complaint with the Secretary of the U.S. Department of Health and Human Services. Contact the Facility Privacy Official for additional information.

Signature of Privacy Official

Date

Print name

If your request to copy the requested information has been granted, you will be charged a reasonable fee for photocopying and mailing.

Distribution of copies: Original to patient's Medical Record, copy to patient.

Express Health Clinic Corporation NOTIFICATION OF TIME EXTENSION

Patient Name: _____ Medical Record No: _____

Facility Name: Express Health Clinic Corporation

TYPE OF REQUEST:

____ Request for Access to PHI of former patient

____ Request to Amend PHI

____ Request for an Accounting of Disclosures

Date of original request: _____

Original Due Date: _____

Request to Access: **30 days** from receipt of request.

Request for Amendment or Accounting: No more than **60 days** from receipt of request.

Revised Due Date (may not be more than 30 days from original due date):

Reason that extension of time to respond is needed:

A copy of this *Notice of Time Extension* has been provided to the patient or the patient's personal representative.

Signature of Privacy Official

Date

Print Name

Distribution of copies: Original to patient's Medical Record, copy to patient.

Express Health Clinic Corporation
REVIEW DETERMINATION LETTER

[DATE]

[Patient NAME]

[ADDRESS]

Dear [patient]:

Your request for review of the denial of access to your health information (see attached form) continues to be denied for the following reason(s):

You may file a complaint with our Facility by contacting the Privacy Official at _____ (Facility phone number). You also may file a complaint with the Secretary of the U. S. Department of Health and Human Services. Please contact the Privacy Official for further information.

Very truly yours,

[SIGNATURE}

[PRINTED NAME AND TITLE]

CURRENT PATIENT ACCESS TO PROTECTED HEALTH INFORMATION

Purpose

To define *current* patients' right to access their medical records. Access to medical records is a patient right under OBRA regulations. Therefore, the facility must meet the OBRA time frames and other requirements when a current patient requests access. The OBRA requirements are more stringent than the HIPAA Privacy Rule requirements. The facility may not deny access to a current patient, and cannot require the request for access to be in writing.

Policy

Every patient has the right to access his or her protected health information (PHI). The Facility will respond to all requests to access a patient's health information. Some states may have more stringent regulations and it is the responsibility of each facility to research state laws. For current patients, OBRA time lines must be adhered to unless state laws require the Facility to respond in a shorter time frame.

Procedure

Request to View Medical Records:

1. Refer the patient or legal* representative to the Facility designated Health Information Manager/Medical Records Coordinator.
2. Confirm the requestor has the legal authority to view the record by determining who is considered a legal representative based on state law (e.g., guardian, conservator, durable power of attorney).
3. Set up a meeting within 24 hours as required by law. If the requestor cannot accommodate a meeting within the 24 hour time frame, the review should be set up at a mutually agreed upon time.
4. Assure a staff member is in attendance at all times during the meeting, to:
 - a. Answer questions,
 - b. Assure the record is not altered in any way, and
 - c. Assure documents are not removed/destroyed.
5. Allow the patient or legal representative to review and read the record without intervention from the staff member present.
6. Although OBRA does not require the access request to be in writing, the preferred procedure is to complete an *Access to Protected Health Information* form. (See a sample form in the Policy "Former patients' Access to Protected Health Information.")

* "Legal representative" is the same as "personal representative" as defined under HIPAA rules.

Request for a Copy of Medical Records:

1. Refer the patient or legal representative to the Facility designated Health Information Manager/Medical Records Coordinator.
2. Confirm the requestor has the legal authority to view the record by determining who is considered a legal representative based on state law (e.g., guardian, conservator, durable power of attorney).
3. Although OBRA does not require the access request to be in writing, the preferred procedure is to complete an *Access to Protected Health Information* form. (See a sample form in the Policy “Former patients’ Access to Protected Health Information.”)
4. Disclose the Facility’s charge for copying to the patient or legal representative at the time of the request.
5. Provide the patient or legal representative with the copies within two working days.

ACCOUNTING AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

Purpose

patients have the right to receive an accounting of the disclosures of their Protected Health Information (“PHI”) maintained in their Designated Record Set. The following is the process for responding to a patient’s request for an accounting of disclosures of their PHI made by the Facility.

Policy

Each patient may request and receive an accounting of trackable disclosures of PHI made by the Facility. The potential areas where accounting of disclosures applies are listed in the *Notice of Privacy Practices*. The Facility will provide such an accounting, in accordance with the HIPAA Privacy Rule, when requested by a patient or a patient’s personal representative. The requested information will not include PHI released or disclosed on or prior to April 13, 2003.

Records of disclosures are retained for a six-year period.

Procedure

1. Upon receiving an inquiry from a patient, the Facility Privacy Official provides the patient or personal representative with a copy of a *Request for an Accounting of Disclosures of PHI* (“Request”) form. (See sample *Request* form following this Policy.)

Requests are not evaluated until the *Request* form is completed and signed by the patient or personal representative.

2. The Facility Privacy Official reviews and processes the request.

3. The Facility provides a written accounting no later than 60 days after receipt. If the Facility is unable to meet the 60-day time frame, the Facility may extend the time once by no more than 30 days as long as the individual is provided with a written statement of the reasons for the delay and the date by which the Facility will provide the accounting. (See the *Notification of Time Extension* form in the Policy “Former patient’s Access to Protected Health Information.”)

4. A written accounting is provided to the requestor using an *Accounting of Disclosures* log. (See log following this Policy.)

a. The accounting will include disclosures during the period specified by the patient or personal representative in the request. The specified period may be up to six years prior to the date of the request. Disclosures made on or before April 13, 2003 will not be included in the accounting.

b. The Facility will include known disclosures made by its Business Associates, if aware of any such disclosures required to be included in an accounting.

c. For each disclosure, the accounting will include:

i. Date the request for disclosure was received;

ii. Name of entity requesting disclosure and, if known, the address of such person or entity;

- iii. A brief description of the PHI that was disclosed; and
 - iv. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure.
- d. If there are multiple disclosures for health oversight or law enforcement officials for a single purpose, the Facility may provide:
- i. The first disclosure during the accounting period;
 - ii. The frequency, or number of disclosures made during the accounting period;
 - iii. The date of the last such disclosure during the accounting period.
5. For disclosures of PHI for research purposes in a project consisting of fifty or more individuals, the accounting may provide:
- a. Name of protocol or other research activity;
 - b. Description and purpose of research, criteria for selecting particular records;
 - c. Brief description of the type of PHI disclosed;
 - d. Date or period of time during which disclosure(s) occurred, including date of last disclosure during accounting period;
 - e. Name, address, telephone number of entity that sponsored the research and of the researcher to whom the information was disclosed;
 - f. Statement that PHI of the patient may or may not have been disclosed for a particular protocol or the research activity.
6. The Facility will provide the first accounting to a patient or personal representative within a 12-month period without charge. However, the Facility may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same party within the 12-month period, provided the Facility has informed the requesting party of the charges in advance, giving the party the opportunity to withdraw or modify the request.
7. The Facility may exclude those disclosures that qualify as an exception.
8. The Facility must document and retain for six years from the date of the accounting:
- a. The information required to be included in the accounting, and
 - b. The written accounting provided to the requesting party.

Potential Areas where Accounting of Disclosures Applies:

1. Disclosures to Public Health Authorities

- For the purpose of preventing or controlling disease, injury or disability
- To conduct public health surveillance
- For public health investigations and interventions
- For reporting vital events such as births and deaths

- To a foreign government agency at the request of a public health authority
- To report child/elder abuse
- If necessary, to prevent or lessen a serious and imminent threat to the health or safety of an patient or the public

2. *Disclosures to an Entity Subject to the Food and Drug Administration*

- To report adverse events, product defects or biological product deviations
- To track products
- To enable product recalls, repairs or replacements
- To conduct post marketing surveillance

3. *Disclosures to an Employer*

- Only PHI specific to a work-related illness or injury, and
- Required for the employer to comply with its obligations under federal or state occupational safety and health laws

4. *Disclosures to Health Oversight Agencies*

- For government benefit program eligibility
- To determine compliance with civil rights laws
- For civil, administrative or criminal investigations, proceedings or actions

5. *Disclosures in Judicial and Administrative Proceedings*

- In response to a court order or court ordered warrant
- In response to a subpoena, only if approved by Privacy Officer and the Legal Department

6. *Disclosures to Law Enforcement Officials*

- For the purpose of locating a suspect, fugitive, material witness or missing person
- About a patient who is or is suspected to be a victim of a crime
- Regarding crimes on the Facility premises
- Regarding suspicious deaths
- In response to an administrative request, civil investigative demand or grand jury subpoena, after review by Privacy Officer and the Legal Department
- For the purpose of averting a serious threat to health or safety

7. *Disclosures about victims of abuse, neglect or domestic violence*

- To a government authority authorized by law to receive reports of abuse, neglect or domestic violence

8. *Disclosure of Deceased Persons' PHI*

- To the Coroner, Medical Examiner or Funeral Directors
- To organ procurement organizations

9. *Disclosures for research*

- Only if disclosure was made without an authorization as permitted by the Privacy rule

10. *Disclosures for Specialized Government Functions*

- To Armed Forces personnel for military purposes
- To authorized federal officials for the protection of the Patient and other Federal officials
- To other government agencies, if approved by Privacy Officer and the Legal Department

11. *Disclosures for Worker's Compensation*

- As authorized by and to the extent necessary to comply with the law

Exceptions to Accounting of Disclosures:

Accounting of disclosure does not include disclosures:

- Necessary to carry out treatment, payment, and health care operations
- To the patient for whom the PHI was created or obtained
- Pursuant to a signed authorization by the patient or personal representative
- For the Facility's Directory or to persons involved in the patient's care or other notification purposes
- For national security or intelligence purposes
- To a correctional institution
- Temporarily suspended by a law enforcement official or health oversight agency (exception applies only during the period of suspension)
- That are incidental
- As part of a Limited Data Set
- That occurred on or prior to April 13, 2003

Express Health Clinic Corporation
REQUEST FOR AN ACCOUNTING OF DISCLOSURES
OF PROTECTED HEALTH INFORMATION

Patient's Name: _____ Medical Record Number: _____

Patient's Date of Birth _____ Facility's Name: Express Health Clinic Corporation

Date Range to be Included

I would like an accounting of disclosures of my Protected Health Information (PHI) for the following time frames.

(Please note the maximum time frame that can be requested is six years prior to the date of this request.)

From Date _____ To Date _____

From Date _____ To Date _____

From Date _____ To Date _____

Fees

First request in a 12-month period: Free

Subsequent Requests: _____ (Cost-based fee per entity)

I understand that there may be a fee for this accounting and wish to proceed. I also understand that the accounting will be provided to me within 60 days unless I am notified in writing that an extension of up to 30 days is needed.

Qualified Exceptions to the Accounting

I understand that, by law, the Facility is not required to account for disclosures that meet the following criteria:

- The disclosure was necessary to carry out treatment, payment, and health care operations.
- The disclosure was to the patient for which the PHI was created or obtained.
- The disclosure was pursuant to a signed authorization by the patient or personal representative.
- The disclosure was for the Facility's directory or to persons involved in the patient's care or other notification purposes.

- The disclosure was for national security or intelligence purposes.
- The disclosure was to a correctional institution or law enforcement official.
- The disclosure occurred prior to April 13, 2003.

Signature of patient or Personal Representative

Date

Distribution of copies: Original to patient's Medical Record, copy to patient

AMENDMENT OF PROTECTED HEALTH INFORMATION

Purpose

This Policy is to provide a process for responding to a patient's request for an amendment to Protected Health Information ("PHI").

Policy

A patient has the right to request that the Facility amend his PHI maintained in the Designated Record Set for as long as the PHI is maintained. The policy of this Facility is to respond to a patient's request for amendment of PHI in accordance with the HIPAA Privacy Rule. This policy contains the procedures for approving an amendment, denying an amendment and making an amendment at the request of another covered entity.

Note: The *Notice of Privacy Practices* states that an amendment is not necessary to correct clerical errors.

Procedure

1. The patient will be notified of the right to amend his PHI in the *Notice of Privacy Practices*.
2. The Facility Privacy Official ("Privacy Official") will process all requests for amendment.
3. Upon receiving an inquiry from a patient regarding the right to amend his/her PHI, the Privacy Official will provide the patient with a copy of an *Amendment of Protected Health Information* ("*Amendment of PHI*") form. A request for amendment will not be evaluated until the request form is completed and signed by the patient or personal representative.

(See sample *Amendment of PHI* form following this Policy.)

Evaluating and Responding to the Request for Amendment

1. The Privacy Official will date stamp or write the date received and initial the *Amendment of PHI* form.
2. The Privacy Official will make a determination to accept or deny the amendment after consultation with the appropriate staff, if needed.
3. The Privacy Official shall act on the request for amendment no later than 60 days after receipt of the request.
 - a. If the amendment is accepted, Facility staff shall make the amendment and inform the patient within 60 days of the written request.
 - b. If the amendment is denied, the Facility shall notify the patient in writing of the denial within 60 days of the written request.
4. If the Facility is unable to act on the request for amendment within 60 days of receipt of the request, it may have one extension of no more than 30 days. The Privacy Official will notify the patient in writing of the extension, the reason for the extension and the date by which action will be taken. (See the sample *Notification of Time Extension* in the Policy "Former patient's Access to Protected Health Information.")

Denial of Request for Amendment

1. The Facility may deny the request for amendment in whole or in part if:
 - a. The PHI was not created by the Facility (i.e., an Advance Directive). An exception may be granted if the patient provides a reasonable basis to believe that the creator of the PHI is no longer available to act on the requested amendment and it is apparent that the amendment is warranted. For example, a hospital or clinic, which has given the Facility information on a patient, has since closed its doors and left no means of obtaining its past information or records that were destroyed by fire or flood with no backup copies available.

Note: This should rarely be the case. Every other avenue will be explored before an amendment is made to information that was not created by the Facility.
 - b. The PHI is not part of the Designated Record Set (i.e., information gathered on worksheets or daily communication sheets that do not become a part of the Medical Record and are not retained).
 - c. The PHI would not be available for inspection under the HIPAA Privacy Rule.
 - d. The PHI that is subject to the request is accurate and complete.
2. If the Privacy Official, in consultation with the appropriate staff, determines that the request for amendment is denied in whole or in part, the Privacy Official will provide the patient with a timely amendment denial letter. The denial shall be written in plain language and shall contain:
 - a. The basis for the denial;
 - b. A statement that the patient has a right to submit a written statement disagreeing with the denial and an explanation of how the patient may file such statement;
 - c. A statement that, if the patient does not submit a statement of disagreement, the patient may request that the Facility include the patient's request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment;
 - d. A description of how the patient may file a complaint with the Facility or to the Secretary of the U.S. Department of Health and Human Services. The description must include the name or title and telephone number of the contact person for complaints. (See the Policy "Complaints.")
3. The patient may submit a written statement of disagreement.
4. If the patient submits a written statement of disagreement, the Facility may prepare a written rebuttal to the statement. The Facility shall provide a copy of the written rebuttal to the patient who submitted the statement.
5. The following documentation must be appended (or otherwise linked) to the PHI that is the subject of the disputed amendment:
 - a. The patient's *Amendment of PHI* form;
 - b. The Facility's amendment denial letter;
 - c. The patient's statement of disagreement, if any; and

- d. The Facility's written rebuttal, if any.

Future Disclosures of PHI that is the Subject of the Disputed Amendment

1. If the patient submitted a statement of disagreement, the Facility will disclose all information listed in Item 5. above or an accurate summary of such information with all future disclosures of the PHI to which the disagreement relates.
2. If the patient did not submit a statement of disagreement, and if the patient has requested that the Facility provide the *Amendment of PHI* form and the amendment denial letter with any future disclosures, the Facility shall include these documents (or an accurate summary of that information) with all future disclosures of the PHI to which the disagreement relates.

Acceptance of the Request for Amendment

If the Facility accepts the requested amendment, in whole or in part, the Facility will take the following steps:

1. The Facility Privacy Official shall place a copy of the amendment in the patient's Medical Record or provide a reference to the location of the amendment within the body of the Medical Record.
2. The Privacy Official shall notify the relevant persons with whom the amendment needs to be shared, as identified by the patient on the original *Amendment of PHI* form.
3. The Privacy Official shall identify other persons, including Business Associates, that it knows have the PHI and that may have relied on, or could foreseeably rely on, such information to the detriment of the patient. The Privacy Official will inform the patient of, and obtain the patient's agreement to notify such other persons or organizations of the amendment.
4. The Privacy Official shall make reasonable efforts to inform and provide the amendment within a reasonable time to:
 - a. Persons identified by the patient as having received the PHI and needing the amendment;
 - b. Persons, including Business Associates, that the Facility knows have the PHI and may have relied, or could foreseeably rely, on such information to the detriment of the patient.
5. If no additional persons needing notification of the amendment are identified, the Privacy Official shall inform the patient in writing that the amendment has been accepted.

Actions on Notices of Amendment

If another Covered Entity notifies the Facility of an amendment to PHI it maintains, the Privacy Official shall make the amendment to the patient's Designated Record Set.

1. Amendments to the Designated Record Set shall be filed with that portion of the PHI to be amended.
2. Amendments that cannot be physically placed near the original PHI will be filed in an appropriate location.
3. If it is not possible to file the amendment(s) with that portion of the PHI to be amended, a reference to the amendment and its location will be added near the original information location.
4. If the actual amendment is not in an easily recognized location near the original information, the reference should indicate where it could be found.

5. General information regarding requests for amendment, forms relating to amendments and correspondence relating to denial or acceptance of requests to amend will be filed in the patient's Medical Record.

(See sample Acceptance, Denial, and Notification letters following this Policy.)

Express Health Clinic Corporation

AMENDMENT OF PROTECTED HEALTH INFORMATION

Date Received: _____

Initials of Privacy Official: _____

SECTION A: patient to complete the following information

Date: _____

Patient Name: _____ Medical Record Number _____

Patient Date of Birth: _____

Address: _____

REQUEST:

I hereby request that the Facility amend the following in my Designated Record Set (**check all that apply**):

_____ My Medical Records

_____ My Business Office Files

Date(s) of information to be amended (i.e., date of visit, treatment, or other health care services)

The information is incorrect or incomplete in the following manner:

I request this amendment for the following reason(s):

The information should be amended as follows:

I understand that Express Health Clinic Corporation may or may not supplement my record with an addendum based on my request. I also understand that Express Health Clinic Corporation is not able to alter the original documentation in a record under any circumstances. Regardless whether my request is granted or denied, I understand that this request will be made a part of my permanent Medical Record and will be sent as part of the Medical Record in response to any authorized requests for release of my Protected Health Information.

Signature of Patient or Personal Representative

Date

Print Name

Personal Representative's Title (e.g., Guardian, Executor of Estate, Health Care Power of Attorney)

AMENDMENT OF PROTECTED HEALTH INFORMATION - *side 2*

SECTION B: Facility to complete the following

Date of Receipt of Request _____

Request for correction / amendment has been: _____ Accepted _____ Denied

If denied, check reason for denial:

_____ The PHI was not created by this Facility.

_____ The PHI is not part of patient's Designated Record Set.

_____ The PHI is not available to the patient for inspection as required by federal law (i.e., psychotherapy notes)

_____ The PHI is accurate and complete.

NOTICE TO PATIENT/OTHERS:

Patient and/or others notified of determination via one or more of the following (**check all that apply**):

_____ *Amendment Acceptance Letter* sent to patient on _____ (date).

_____ *Amendment Acceptance with Consent to Notify* sent to patient on _____ (date).

_____ *Notification of Amendment* sent to identified persons pursuant to patient authorization on _____ (date).

Signature of Privacy Official

Date

Print Name

Distribution of copies: Original to patient's Medical Record, copy to patient

Express Health Clinic Corporation
AMENDMENT ACCEPTANCE LETTER

[Date]

[patient NAME]

[ADDRESS]

Dear [patient]:

Your request to amend your Protected Health Information (see attached form) has been approved. We will notify the individuals and/or organizations that you identified in the original amendment request.

Very truly yours,

[AUTHOR SIGNATURE]

[PRINTED NAME AND TITLE]

Express Health Clinic Corporation

AMENDMENT ACCEPTANCE WITH CONSENT TO NOTIFY LETTER

[DATE]

[patient NAME]

[ADDRESS]

Dear [patient]:

Your request to amend your Protected Health Information (see attached form) has been approved. We will notify the individuals and/or organizations that you identified in the original amendment request.

In addition, we have identified the following individuals and/or organizations that received your Protected Health Information. We are not permitted to notify these individuals and/or organizations without your written agreement. If you would like us to notify the individuals and/or organizations listed below, you must sign, date, and return this statement to us.

Very truly yours,

[AUTHOR SIGNATURE]

[PRINTED NAME AND TITLE]

I hereby request and consent to the notification of the above-identified persons and/or organizations who have previously received my Protected Health Information regarding the approval of my request for amendment.

Signature of Patient or Personal Representative

Date

Print Name

Personal Representative's Title (e.g., Guardian, Executor of Estate,
Health Care Power of Attorney)

Express Health Clinic Corporation
NOTIFICATION OF AMENDMENT LETTER

[DATE]

[Name of Individual/Organization to Receive *Notification of Amendment*

[ADDRESS]

Re: [patient]

Approval of Amendment of Protected Health Information

Dear [RECIPIENT]

We have agreed to a request from the above-referenced patient to amend his/her Protected Health Information as outlined on the attached form entitled “*Amendment of Protected Health Information.*”

In compliance with the HIPAA Privacy Rule (45 CFR §164.526—Amendment of Protected Health Information), we are providing you with proper notification of this approved amendment.

Thank you.

Very truly yours,

[AUTHOR SIGNATURE]

[PRINTED NAME AND TITLE]

Express Health Clinic Corporation
AMENDMENT DENIAL LETTER

[DATE]

[patient NAME]

[ADDRESS]

Dear [patient]:

Your request to amend your Protected Health Information (see attached form) has been denied for the following reason(s):

You have the right to submit a written statement disagreeing with the denial. If you choose to do so, submit your statement to the Facility Privacy Official.

If you do not submit a statement of disagreement, you may request that the Facility include your request for amendment and the denial in any future disclosures of your Protected Health Information.

You may file a complaint with our Facility by contacting the Facility Privacy Official at _____ (Facility phone number). You also may file a complaint with the Secretary of the U.S. Department of Health and Human Services. Please contact the Facility Privacy Official for contact information.

Very truly yours,

[SIGNATURE]

[PRINTED NAME AND TITLE]

ALTERNATIVE COMMUNICATION OF PROTECTED HEALTH INFORMATION

Purpose

To ensure the patient's right to request that communications of Protected Health Information ("PHI") be delivered by alternative means or at alternate locations.

Policy

A patient will be allowed to request that the Facility communicate PHI to him by alternative means or at alternative locations. The Facility shall accommodate reasonable requests.

Procedure

1. The patient will be notified of the right to request communication by alternative means or at alternative locations in the Facility's *Notice of Privacy Practices*.
2. The Facility Privacy Official will manage requests to receive communications by alternative means.
3. When an inquiry is received from a patient regarding the right to request that the Facility communicate with him or his personal representative by some alternate means, the Facility will provide the patient with a copy of A *Request for Communications by Alternative Means* ("*Request for Communications*") form. A request will not be evaluated until this request form is completed and signed by the patient or personal representative.

(See sample *Request for Communications* form following this Policy.)

4. The Privacy Official will review the completed *Request for Communications* form to determine if it is a reasonable request. The Facility may not require an explanation for the request. The Facility's decision will not be based on the perceived merits of the request. The Facility will accommodate a request determined to be reasonable.
5. The Privacy Official will complete the Response section of the *Request for Communications* form to inform the patient of the Facility's decision.
6. The Privacy Official shall maintain all requests and responses in the appropriate location in the patient's Medical Record. (See the Policy "Retention of Protected Health Information.")

Express Health Clinic Corporation

REQUEST FOR COMMUNICATION BY ALTERNATIVE MEANS/LOCATION

Patient Name: _____ Medical Record Number _____

Patient Date of Birth: _____

Patient Address: _____

Facility Name: Express Health Clinic Corporation

I wish to receive communication of my Protected Health Information from the Facility by the following mean:

Signature of Patient or Personal Representative

Date

Print Name

Personal Representative's Title (e.g., Guardian, Executor of Estate, Health Care Power of Attorney)

Response to Request

Date Request Received: _____

Alternative communication has been:

____ Accepted

____ Declined: The request is not reasonable because:

Signature of Privacy Official

Date

Print Name

Distribution of copies: Original to patient's Medical Record, copy to patient

COMPLAINTS SECTION

Purpose

To ensure that an effective complaint process is in place to deal with privacy violations. The process is to include:

- Identification of a privacy designee who is responsible for receiving complaints.
- A method for documenting receipt of complaints and their resolution.
- Assurance that no individual will be required to waive their rights to file a complaint with the Department of Health and Human Services.

Policy

It is the policy of this Facility to ensure the privacy of Protected Health Information (“PHI”) as well as to ensure that such information is used and disclosed in accordance with all applicable laws and regulations. Any concerned individual has the right to file a formal complaint concerning privacy issues without fear of reprisal. Such issues could include, but are not limited to, allegations that:

- PHI that was used/disclosed improperly;
- Access or amendment rights were wrongfully denied; or
- The Facility’s *Notice of Privacy Practices* does not reflect current practices accurately.

Procedure

1. All patients or their personal representatives will be notified of their right to complain to the Facility or the Department of Health and Human Services in the Facility’s *Notice of Privacy Practices*.
2. All concerns may be registered by telephone, mail, or in person.
3. Upon receipt of a complaint about a Facility’s privacy policies or its compliance with those policies or the law, the complaint will be recorded on a *Complaint Log* or *Complaint Regarding Use or Disclosure of Protected Health Information* (“*Complaint*”) form. (See sample *Complaint* form and *Complaint Log* following this Policy.)
4. The Facility Privacy Official will review the *Complaint* form/log to ensure that the information is complete, and take the necessary steps to get complete information:
 - a. Document the date, time, and name of the person making the complaint in the *Complaint Log*.
 - b. Investigate the complaint.
 - c. Document the resolution of the complaint.
5. Once the *Complaint* form/log is completed correctly, the Facility Privacy Official will review and investigate the complaint to determine if a violation of the law or Facility policies has occurred.
6. Following this review, the Facility Privacy Official shall submit his or her findings to the Privacy Officer for final review.

(See sample *Resolution of Complaint Regarding Uses/Disclosures of PHI* form following this Policy.)

7. The Privacy Officer shall determine the substance of the findings and will direct the Facility Privacy Official as to the content and method of response:

- a. Document the resolution of the complaint.
- b. Communicate the outcome of the complaint with the individual filing the complaint within 30 days from receipt of complaint.

8. The Facility Privacy Official shall maintain documentation of all complaints received and their disposition for a period of at least six years (from the date of creation) in accordance with federal regulations.

Express Health Clinic Corporation
COMPLAINT REGARDING USES/DISCLOSURES
OF PROTECTED HEALTH INFORMATION

Tracking Number _____

This form is to be used to file a complaint with the Facility regarding its privacy policies and procedures, and its compliance with those policies and procedures or the federal Privacy Rule.

When this form is complete, please return it to:

Patient Information

Patient Name _____ :

Requestor Name (if not the patient): _____

Address: _____

Date of Birth _____ Social Security Number: _____

Date of Incident: _____

Location of Incident: _____

Please describe the practice or incident about which you wish to complain:

Name & title of person(s) involved, if known: _____

Please describe why you believe that this practice or incident was improper:

Please attach any documentation that supports your complaint to this form.

I certify that the information recorded above is true to the best of my knowledge, and that I have a good faith belief that such practice or incident is a violation of federal laws regarding the handling of a patient's health information or of the Facility's privacy policies and procedures.

Signature _____ Date _____

Express Health Clinic Corporation
RESOLUTION OF COMPLAINT REGARDING USES/DISCLOSURES
OF PROTECTED HEALTH INFORMATION

Person investigating the complaint:

Name _____

Location _____

Tracking Number: _____

Date _____

Resolution or Conclusion of investigation:

Comments:

Date and Time Resolution Communicated to Individual:

Approval of Privacy Officer

Name _____

Date _____

Comments/Instructions:

Express Health Clinic Corporation

LOG OF INTERNAL COMPLAINTS REGARDING PRIVACY ISSUES

DATE RECEIVED	IDENTITY OF INDIVIDUAL MAKING COMPLAINT (IF KNOWN)	PERSON RECEIVING COMPLAINT	NATURE OF COMPLAINT	STEPS TAKEN TO RESOLVE COMPLAINT	DATE OF RESOLUTION	Method Filed	Tracking Number
Example: 04/30/03	Hotline – anonymous	Pam Peters – privacy officer	Computer screens in clinic not shielded from visitor view	Computer terminals moved to area where they cannot be seen by passerby; monitor screen shields installed	05/02/03		

DATE RECEIVED	IDENTITY OF INDIVIDUAL MAKING COMPLAINT (IF KNOWN)	PERSON RECEIVING COMPLAINT	NATURE OF COMPLAINT	STEPS TAKEN TO RESOLVE COMPLAINT	DATE OF RESOLUTION	Method Filed	Tracking Number

RESTRICTIONS TO PERMITTED USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

Purpose

To provide a process for a patient to request a restriction to an otherwise permitted use or disclosure of the patient's Protected Health Information ("PHI"), and for the Facility to respond to such request.

Policy

A patient has the right to request that otherwise permitted uses and disclosures of PHI be restricted. Specifically, the patient may request restrictions on:

- The use and disclosure of PHI for treatment, payment or health care operations, or
- The disclosures to family, friends or others for involvement in care and notification purposes.

The Facility is not required to comply with such requests for restriction, but will consider and may agree to a restriction. The Facility will consider the need for access to PHI for treatment purposes when considering a request for a restriction. A request for restriction must be made in writing. The Facility Privacy Official ("Privacy Official") will notify the patient of its determination with respect to the request.

Procedure

1. The patient will be notified of the right to request restrictions on the use and disclosure of PHI in the Facility's *Notice of Privacy Practices* and that the request must be in writing.
2. The Privacy Official shall manage requests for restrictions. All documentation associated with this request will be placed in the patient's Medical Record.
3. The Privacy Official will provide the patient a *Request to Restrict Use and Disclosure of Protected Health Information* ("*Request to Restrict*") form if the patient asks to make a restriction.
(See sample *Request to Restrict* form following this Policy.)
4. A request for restriction will not be reviewed until the *Request to Restrict* form is completed and signed by the patient. The Privacy Official may assist the patient in completing the form, if necessary.
5. The Privacy Official will review the request in consultation with other Facility staff to determine the feasibility of the request. The Facility shall give primary consideration to the need for access to the PHI for treatment and payment purposes in making its determination.
6. The Privacy Official shall complete the "Facility Response" section of the *Request to Restrict* form and provide a copy to the patient.

Restriction Not Accepted

If the Facility declines the request for restriction, the Privacy Official will provide the patient with a copy of the signed response (part of the *Request to Restrict* form).

Restriction Accepted

1. If the Facility agrees to the requested restriction, it must abide by the accepted restriction with the following exceptions:
 - a. The Facility may use the restricted PHI, or may disclose such information to a health care provider if:
 - i. The patient is in need of emergency treatment, and
 - ii. The restricted PHI is needed to provide emergency treatment. In this case, the Facility will release the information, but ask the emergency treatment provider not to further use or disclose the patient's PHI.
 - b. The Facility may disclose the information to the individual who requested the restriction.
 - c. The Facility may use and disclose Directory Information unless the patient has objected to such use or disclosure (see the Policy "Uses and Disclosures of Protected Health Information for the Directory").
 - d. The Facility may use and disclose the restricted PHI when statutorily required to use and disclose the information under the HIPAA Privacy Rule.
2. The Privacy Official will notify appropriate Facility staff of the restriction.
3. The Privacy Official will document the restriction on the *Request to Restrict* form, provide the patient with a copy and maintain the original in the patient's Medical Record.

Terminating the Restriction

Termination with the patient's agreement

1. The Facility may terminate the accepted restriction if:
 - a. The patient agrees to the termination in writing; or
 - b. The patient agrees to the termination verbally and the verbal agreement is documented.
2. The Privacy Official will notify the appropriate Facility staff of the termination of the restriction.
3. The Privacy Official will document the patient's agreement to the termination of the restriction on the *Request to Restrict* form, provide the patient with a copy and maintain the documentation in the patient's record.
4. Termination of a restriction with the patient's agreement is effective for all PHI created or received by the Facility.

Termination without the patient's agreement

1. The Facility may terminate the restriction without the patient's agreement if it informs the patient that the restriction is being terminated.

2. Such termination is only effective with respect to PHI created or received after the Facility has informed the patient that it is terminating the restriction.

Note: The Facility must continue to abide by the restriction with respect to any PHI created or received before it informed the patient of the termination of the restriction.

3. Inform by mail: If the patient is informed by mail that the Facility is terminating the restriction, the notification shall be sent via certified mail, return receipt requested. The Facility shall maintain a copy of the notification and of the return receipt with the *Request to Restrict* form. The Facility shall not terminate the restriction until it receives confirmation that the patient has received the notification.

4. Inform in person: It is preferable to have the patient sign and date a notification of termination of a restriction. However, it will be acceptable to document that the patient was so notified on the *Request to Restrict* form.

5. Inform via telephone: If the patient is informed by telephone, this action shall be documented on the *Request to Restrict* form. In addition, a letter shall be sent via certified mail, return receipt requested. The termination shall be effective as of the date the patient is informed by telephone.

Express Health Clinic Corporation
REQUEST TO RESTRICT USE AND DISCLOSURE
OF PROTECTED HEALTH INFORMATION

Patient Name: _____ Medical Record No: _____

Patient Date of Birth: _____

Address: _____

Facility Name: Express Health Clinic Corporation

Directory Information Restriction: I request that the disclosure of my information maintained in the Facility directory be restricted in the following manner:

_____ Do not include my name, location, general condition or religious affiliation in the Facility directory.

_____ Do not disclose my name or religious affiliation to members of the clergy.

_____ Do not disclose my location in the building to: _____.

_____ Do not disclose my general condition to: _____.

Signature of Patient or Personal Representative

Date

Print Name

Personal Representative's Title (e.g., Guardian, Executor of Estate, Health Care Power of Attorney)

Other Restrictions: I request the following restriction(s) on the use or disclosure of my Protected Health Information:

_____ Do not release information to the following person(s):

Other restriction (please specify):

Signature of Patient or Personal Representative

Date

Print Name

Personal Representative's Title (e.g., Guardian, Executor of Estate, Health Care Power of Attorney)

**REQUEST TO RESTRICT USE AND DISCLOSURE OF PROTECTED
HEALTH INFORMATION - side 2**

FACILITY RESPONSE:

_____ Your request for restriction has been declined.

Note: The Facility may not deny a request for restriction of Directory Information.

_____ Your request for restriction has been accepted. In the case of an emergency or if necessary to comply with the law, we may use and disclose your health information in violation of the restriction. Other than in those circumstances, we will abide by your request unless and until the restriction is terminated (with or without your agreement) and you are notified.

Signature of Facility Privacy Official _____
Date

Print Name

TERMINATION OF RESTRICTION

_____ The above name patient agreed to terminate this restriction on: _____.

_____ The above named patient was notified on _____ (date) that this restriction was terminated.

patient was notified: (check appropriate box) :

_____ In person

_____ By telephone (attach documentation of notification)

_____ By mail (attach documentation of notification)

Signature of Facility Privacy Official _____
Date

Print Name

Distribution of copies: Original to patient's Medical Record; copy to patient.

OTHER REQUIREMENTS SECTION

BUSINESS ASSOCIATES

Purpose

The purpose of this Policy is to provide a process for establishing a written agreement with each of the Facility's Business Associates ("BA") as required by the HIPAA Privacy Rule.

Policy

The Facility contracts with various outside entities and organizations to perform functions or provide services on behalf of the Facility that may involve the disclosure of Protected Health Information ("PHI") to the outside entity. These outside entities are the Facility's Business Associates. The policy of this Facility is to obtain written assurances from BAs that they will appropriately safeguard any PHI they create or receive on the Facility's behalf. Such written assurances will be in place before the Facility discloses PHI to the Business Associate.

Procedure

1. The Facility Administrator will follow established procedures regarding contract review, revision and approval to assure that contract is in compliance with state and federal law.
2. For each contract, determine whether a Business Associate Agreement is necessary. (See the "Business Associate Decision Tree" following this Policy.) Common examples of BAs are:
 - a. The Facility's Medical Director
 - b. The Facility's consultants that conducts reviews to assist the Facility with regulatory compliance
 - c. An attorney who reviews patient information to assist in the appeal of a survey citation or any other matter that requires the disclosure of PHI to the attorney
 - d. Medical Records Consultant

Note: Business Associate language is *not* required when the BA is a health care provider and all disclosures to the BA concern the treatment of a patient.
3. If a BA Agreement is necessary and the third party provides its own BA Agreement, review the Agreement to assure it meets all requirements of the Privacy Rule. (See "Business Associate Checklist" following this Policy.)
4. If a BA Agreement is necessary, and the third party does not provide the Agreement, submit Facility's template BA Agreement for approval by the third party.
5. If the BA refuses to sign the BA Agreement, the HIPAA Privacy Rule prohibits the Facility from disclosing any PHI to the BA. If the BA requires access to PHI in order to perform the function or service on behalf of the Facility, the Facility shall not contract with the BA.
6. The original signed contract and contract addendum containing BA language shall be maintained by the Facility.
7. Violations of BA Requirements - If Facility staff learns of a breach or violation of a BA requirement by a BA, such breach or violation shall be reported to the Privacy Officer, his designee, or

to the Compliance Department. The Privacy Officer or Compliance Designee will assist the Facility in determining whether reasonable steps can be taken to cure the breach. If the Facility's reasonable steps to cure the BA's violations are unsuccessful, the Facility may:

- a. Terminate the contract or arrangement; or
- b. If termination is not feasible, report the problem to the Secretary of the U. S. Department of Health and Human Services.

8. Notice of Termination of a Contract with a BA - The Facility shall notify the Privacy Officer, his designee or the Legal Department when issuing or receiving a notice of contract termination involving a BA. The Legal Department will assist with contacting the BA regarding the BA's obligations to return or destroy all PHI or, if return or destruction is not feasible, to extend the protections of the BA requirements to the PHI and to limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible.

The contract and contract addendum must be retained for six years after the contract was last in effect.

Express Health Clinic Corporation
BUSINESS ASSOCIATE CHECKLIST

Contract Provision	Reg. Cite	Requirement	Related provisions, comments
	164.504(e)(2)(i)	Establish permitted and required uses and disclosures of PHI by BA	Final rule – must generally state purposes, reasons for use/disclosure and types of persons to whom info can be disclosed
	164.504(e)(2)(i)(A)	May permit BA to use or disclose PHI for “proper management & administration of BA as permitted by (e)(4)	
	164.504(e)(4)(i)(A) and (B)	May permit BA to use PHI – in its capacity as a BA if necessary for the proper management & administration of BA or to carry out the legal responsibilities of BA.	
	164.504(e)(4)(ii)(B)(2)	The person to whom the information was disclosed notifies BA of any instance of which it is aware in which the confidentiality of the information has been breached.	
	164.504(e)(2)(i)(B)	BA may provide data aggregation services relating to the health care operations of the covered entity.	
	164.504(e)(2)(ii)(A)	BA will not use or further disclose the information other than as permitted or required by the contract or as required by law.	
	164.504(e)(2)(ii)(B)	BA will use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract.	
	164.504(e)(2)(ii)(C)	BA will report to the CE any use or disclosure of the information not provided for by its contract of which it becomes aware.	Negotiate time and manner of reporting with BA – in writing, to whom,

Contract Provision	Reg. Cite	Requirement	Related provisions, comments
			time frame, etc.
	164.504(e)(2)(ii)D	BA will ensure that any agents, including a subcontractor, to whom it provides PHI received from, or created or received by the BA on behalf of, the CE agrees to the same restrictions and conditions that apply to the BA with respect to such information.	May want BA to list subcontractors and agents in exhibit.
	164.504(e)(2)(ii)E	<u>Access:</u> BA will make available PHI in accordance with 164.524.	Not necessary if BA does not have PHI in a designated record set.
	164.504(e)(2)(ii)F	<u>Amendment:</u> BA will make available PHI for amendment and incorporate any amendments to PHI in accordance with 164.526.	Not necessary if BA does not have PHI in a designated record set.
	164.504(e)(2)(ii)G	<u>Accounting:</u> BA will document disclosures of PHI as would be required for CE to respond to a request for an accounting.	
	164.504(e)(2)(ii)G	<u>Accounting:</u> BA will make available PHI to provide an accounting of disclosures in accordance with 164.528.	
	164.504(e)(2)(ii)H	BA will make internal practices, etc. available to the Secretary.	
	164.504(e)(2)(ii)I	<u>Termination:</u> BA will – if feasible – return or destroy all PHI received from, or created or received by the BA on behalf of the CE. BA will retain no copies of such information. If return or destruction of such information is not feasible, BA will extend the protections of the K to the information and limit further uses and disclosures to those purposes that make the return or the destruction of the information infeasible.	
	164.504(e)(2)(iii)	Authorize termination by CE if CE determines that the BA has violated a material term of the contract.	

Contract Provision	Reg. Cite	Requirement	Related provisions, comments
	Not required by Privacy Rule	<u>Mitigation</u>	Not required by law, but included in sample language in August final rule.
	Not required by Privacy Rule	Insurance	If main contract has insurance clause, may not be necessary in addendum.
	Not required by Privacy Rule	<u>Inspection</u> Allow CE to inspect BA's systems, books, records if CE becomes aware of a breach	CE is not required to monitor BA's activities for Privacy Rule purposes.
	Not required by Privacy Rule	<u>Indemnification</u>	If main contract has indemnification clause, may not be necessary in addendum.
	Not required by Privacy Rule	<u>Interpretation/ambiguity</u> – broadly as necessary to implement and comply with the Privacy Rule and applicable state laws. Any ambiguity shall be resolved in favor of a meaning that complies and is consistent with the Privacy Rule.	
	Not required by Privacy Rule	<u>Amendment to comply with law - Modification of K to be in compliance with Privacy Rule</u>	
	Not required by Privacy Rule	<u>Assistance in litigation or administrative proceedings</u>	If main contract has this type of clause, may not be necessary in addendum.
	Not required by Privacy	<u>Conflict with contract</u> – addendum controls as it relates	

Contract Provision	Reg. Cite	<i>Requirement</i>	<i>Related provisions, comments</i>
	Rule	to PHI	

DEIDENTIFICATION OF PROTECTED HEALTH INFORMATION

Purpose

To convert individually identifiable Protected Health Information (“PHI”) into information that no longer reveals the identity of any patient.

Policy

When patient PHI is used or disclosed for purposes other than treatment, payment or health care operations and/or without patient or personal representative authorization, the PHI must be converted into a format that does not identify the patient. This conversion process is called de-identification of PHI.

The Health Insurance Portability and Accountability (HIPAA) Privacy Rule does not apply to de-identified health information.

The Facility meets the de-identification standard if it has removed all of the required identifiers and if the Facility has no actual knowledge that the information could be used to identify a patient.

Procedure

1. The Facility will convert patient PHI into a format that does not identify the patient (de-identify) when:
 - a. PHI is used or shared for purposes other than treatment, payment or health care operations, or
 - b. Information is used or shared without patient authorization.
2. The Facility will de-identify the PHI by one of the following methods:
 - a. Elimination of all identifiers:
 - i. Names.
 - ii. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code and their equivalent geocodes, except for the initial three digits of a zip code if the geographic area contains more than 20,000 people. If less than 20,000 people are found to be in this area based on the first three digits of the zip code, the code must be changed to 000.
 - iii. All elements of dates (except year) for date directly related to a patient including birth date, admission date, discharge date, date of death: and all ages over 90 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
 - iv. Telephone numbers.
 - v. Fax numbers.
 - vi. Electronic mail address.
 - vii. Social security numbers.

- viii. Medical Record numbers.
- ix. Health plan beneficiary numbers.
- x. Account numbers.
- xi. Certificate/license numbers.
- xii. Vehicle identifiers and serial numbers, including license plate numbers.
- xiii. Device identifiers and serial numbers.
- xiv. Web Universal Resource Locators (URLs).
- xv. Internet Protocol (IP) address numbers.
- xvi. Biometric identifiers, including finger and voiceprints.
- xvii. Full face photographic images and any comparable images.
- xviii. Any other unique identifying number, characteristic, or code.

Note: In addition to removing the above identifiers, the Facility must not have actual knowledge that the information could be used alone or in combination with other information to identify a patient who is a subject of the information.

- b. Statistical De-Identification: A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable applies such principles and determines that the risk is very small that the information could be used to identify the patient. The methods and the results of the analysis must be documented.

3. Re-Identification: The Facility may assign a code that would allow the information to be re-identified by the Facility as long as the code is not derived from or related to information about the patient and is not otherwise capable of being translated so as to identify the patient. The Facility must not use or disclose the code or any other means of record identification for any other purpose and must not disclose the mechanism for re-identification.

MARKETING AND FUNDRAISING

Purpose

To ensure that all marketing and fundraising communications comply with the HIPAA Privacy Rule's requirements, as well as any applicable state laws or regulations. The goal is for the Facility to safeguard the patient's Protected Health Information ("PHI") when engaging in permitted marketing or fundraising activities.

Policy

Marketing communications utilizing PHI require a prior written authorization from the patient with certain defined exceptions.

Fundraising communications that are made specifically for the benefit of the Facility and contain only demographic information and dates of service do not require an authorization as long as the Facility's *Notice of Privacy Practices* describes this limited use of PHI. Fundraising materials must describe how an individual can opt out of receiving future fundraising communications and the Facility must make reasonable efforts to comply with opt-out requests.

Procedure

Marketing

1. The Privacy Rule defines marketing as a communication and/or disclosure of PHI that encourages an individual to use or purchase a product or service, except under the following conditions:
 - a. Communications made directly by the Facility to describe s health related product or service it provides.
 - b. Communications made for treatment of the individual.
 - c. Communications for case management or care coordination for the patient.
 - d. Communications to direct or recommend alternative treatments, therapies, and health care providers or settings of care.
 - e. Face to face communications made by the Facility representative to an individual.
 - f. Promotional gifts of nominal value (defined in policy; for example, less than \$25 each gift not to exceed \$100.00 per annum) provided by the Facility.
2. The Facility must obtain a valid, completed *Authorization to Use or Disclose Protected Health Information* ("Authorization") form prior to using or disclosing PHI for purposes that meet the HIPAA definition of marketing and do not qualify for any of the exceptions listed in Item 1 above.
 - a. The authorization must conform to the authorization policy.
 - b. If direct or indirect remuneration to the Facility from a third party is involved, the authorization must state the nature of such third party remuneration.

3. No authorization is required in the following situations:
 - a. Communications directed at an entire population (not to a targeted individual) that promote health in a general manner and do not endorse a specific product or service;
 - b. PHI is not disclosed in a marketing communication (such as a newspaper advertisement).
4. In the event a planned marketing activity involves payment to the Facility (e.g., cash, referral, gifts, etc.), anti-kickback, inducement, self-referral and general fraud and abuse statutes and regulations may apply. These shall be considered and approved prior to implementation of the marketing activity. The Facility will assure that any marketing activity is in compliance with such laws and regulations.
5. Business Associates and other third parties:
 - a. The Facility may engage a marketing firm to conduct permitted marketing activities on the Facility's behalf. Should the marketing activities require the use or disclosure of PHI to the marketing firm, then a Business Associate relationship would exist and a BA Agreement/Addendum would be required. (See the Policy "Business Associates.")
 - b. The Facility may not sell or disclose PHI to a third party to help the third party market its own products or services without a signed authorization from the patient. (See Policy "Authorization for Release of Protected Health Information.")

Fundraising

1. When fundraising for its own benefit, the Facility may use or disclose without authorization the following PHI to a Business Associate or to an institutionally related foundation, such as a nonprofit charitable foundation to act on the Facility's behalf:
 - a. Demographic information relating to an individual, and
 - b. Dates of health care provided to an individual.
2. The Facility's *Notice of Privacy Practices* must include the following information:
 - a. The Facility or its agent may contact the patient to raise funds for the Facility, and
 - b. The patient may opt out of receiving any fundraising communications.
3. Any fundraising materials the Facility or its agent sends to an individual must describe how the individual may opt out of receiving any further fundraising communications.
4. If the fundraising is not for the Facility's benefit or includes more than demographic or dates of service information, an authorization from the individual is required.

The Facility must make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications

RESPONDING TO A SUBPOENA

Purpose

To ensure that the Facility complies with HIPAA Privacy Rule requirements when a subpoena requesting Protected Health Information (“PHI”) is served.

Policy

Protected Health Information may be disclosed pursuant to judicial or administrative process without the written authorization of the patient, or the opportunity for the patient to agree or object, subject to certain conditions. The Facility will disclose PHI in the course of judicial or administrative process in response to a court or administrative tribunal order. The Facility will disclose PHI in response to a subpoena, discovery request, or other lawful process that is not accompanied by a court order, subject to the conditions set forth in this procedure. In either case, **the Facility will disclose only that PHI expressly authorized by the subpoena, discovery request, other lawful process, or court order.** (The Facility may contact its legal counsel to review and verify the legality of a subpoena requesting PHI served.)

Procedure

1. If the subpoena or other lawful request is accompanied by an order of a court or administrative tribunal, the Facility will verify the identity and authority of the individuals requesting PHI.
2. If the order of the court or other administrative tribunal is valid and meets the verification requirements, the Facility will disclose only that PHI expressly authorized by such order.
3. If the subpoena, discovery request or other lawful process (“subpoena”) is not accompanied by a court order, the Facility will disclose the PHI only after obtaining satisfactory assurances from the party seeking the information that they have made reasonable efforts
 - a. To notify the individual who is the subject of the requested PHI, or
 - b. To secure a qualified protective order.
4. Notice to individual. Prior to disclosing PHI when the subpoena is not accompanied by a court order and there is no qualified protective order meeting the requirements of the Privacy Rule, the Facility will obtain a written statement and accompanying documentation from the requesting party that meets all of the following requirements:
 - a. The written statement and documentation must demonstrate that reasonable efforts have been made to give notice of the request to the individual who is the subject of the requested PHI.
 - b. The notice must contain sufficient information about the litigation or proceeding to permit the individual to raise an objection to the court or administrative tribunal.
 - c. The written statement and accompanying documentation must demonstrate that:
 - i. Time for raising objections to the court or administrative tribunal has elapsed, and

- ii. No objections were filed, or
- iii. The court has resolved all objections filed by the individual or the administrative tribunal and the disclosures being sought are consistent with such resolution.

5. Qualified Protective Order. A qualified protective order means an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

- a. Prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and
- b. Requires the return to the Facility or destruction of the PHI, (including all copies made) at the end of the litigation or proceeding.

6. Prior to disclosing PHI when the subpoena is not accompanied by a court order and the above notice requirements are not met, the Facility will obtain from the requesting party a written statement and accompanying documentation demonstrating that:

- a. The parties to the dispute giving rise to the request for PHI have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute, or
- b. The party seeking the PHI has requested a qualified protective order from such court or administrative tribunal.

7. If the requesting party is unable to meet the requirements for Notice or a Qualified Protective Order, the Facility will notify the requesting party that it is unable to comply with the subpoena. (See sample "Response to a Subpoena" letter following this Policy.)

8. If the requesting party decides to pursue the request for the PHI without meeting the above requirements, the Facility Privacy Official will contact the Facility's Legal Counsel for further direction.

9. The Facility Privacy Official shall document the information regarding the subpoena or other legal process that requests PHI in an *Accounting of Disclosures* Log.

10. The subpoena and any documents produced for the subpoena will be retained according to state and federal regulations.

Express Health Clinic Corporation
RESPONSE TO SUBPOENA NOT ACCOMPANIED BY A COURT ORDER
AND LACKING SATISFACTORY ASSURANCES OF NOTICE
OR QUALIFIED PROTECTIVE ORDER

[Date]

[Attorney Name and Address]

Re: [name of patient]

Dear [Attorney]:

The subpoena you caused to be issued dated _____ requesting copies of protected health information for _____ fails to comply with the applicable requirements of the HIPAA privacy regulations, specifically 45 CFR §164.512(e). As a covered entity, we are allowed to release health information only in accordance with these privacy regulations.

Accordingly, we recommend you either secure an authorization in conformity with 45 CFR 164.508 directly from [name of patient or his/her personal representative] for release of the requested protected health information or take the following steps pursuant to 45 CFR section 164.512(e):

- a) Secure a Court Order detailing your specific needs pursuant to 45 CFR § 164.512(e)(1)(i);
or
- b) Provide us with satisfactory assurance as described at 45 CFR 164.512(e)(1)(ii)(A) that you have made reasonable efforts to notify [name of patient] of your request for protected health information. This requires you to provide us with a written statement and accompanying documentation assuring us that you have made a reasonable effort to provide [name of patient] with a written notice of your request. This written statement you provide to us must also attest that the written notice you provided [name of patient] included:
 - 1. Sufficient information about the litigation or proceeding in which the protected health information is requested to permit [name of patient] to raise an objection to the court or administrative tribunal; and that
 - 2. The time for [name of patient] to raise objections to the court or administrative tribunal has elapsed; and
 - 3. No objections were filed; or
 - 4. All objections filed by [name of patient] have been resolved by the court or administrative tribunal and the disclosures or protected health information being sought are consistent with such resolution; or you may
- c) Provide us satisfactory assurance as described at 45 CFR 164.512(e)(1)(iv) that you have made reasonable efforts to secure a qualified protective order that meets the requirements set forth at 45

CFR 164.512(e)(1)(v). The satisfactory assurance you provide us must include a written statement and accompanying documentation demonstrating that:

1. The parties to the dispute giving rise to the request for protected health information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or
2. The party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal.

A “qualified protective order”, as the term is used in paragraph (c) above means: an order of a court or of an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

- a) Prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and
- b) Requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.

We respectfully ask that if you are not able to meet one of the identified exceptions above regarding disclosure of protected health information, thereby allowing us to release such information in a manner compliant with the regulations cited, that you withdraw your subpoena request until such time as one of the requirements can be met.

Sincerely,

[Privacy Official]

Cc: [Facility Director or administrator]

SANCTIONS

Purpose

To ensure there are appropriate sanctions that will be applied to employees who violate the requirements of the HIPAA Privacy Rule and/or the Facility's HIPAA privacy policies and procedures.

Policy

It is the policy of this Facility to discipline employees who fail to comply with the Facility's policies and procedures regarding HIPAA.

Procedure

1. When a concern arises regarding a possible violation of HIPAA or the Facility's policies or procedures related to HIPAA, the Facility Privacy Official shall begin an investigation promptly. (See the Policy "Complaints" regarding conducting an investigation.)
2. If, at the conclusion of the investigation, it is found that a violation of the Facility's policy or procedure has occurred, the employee involved shall be disciplined in accordance with the severity of the violation and the Facility's disciplinary policy. Violations can be classified according to intent such as:
 - a. Level I Violations are those made accidentally or due to a lack of education.
 - b. Level II Violations are serious violations that are found to show purposeful disregard of Facility policy.
3. The Facility Privacy Official shall review the circumstances surrounding any substantiated violation and take appropriate action to mitigate, to the extent possible, any harmful effects of the violation.
4. Documentation from the investigation shall be given to the Facility Privacy Official to be maintained as a part of the Facility's HIPAA documentation and retained for six years.
5. The disciplinary action report documenting the employee's violation shall be placed in the employee's personnel file as well as a copy provided to the Facility Privacy Official.

VERIFICATION OF IDENTITY AND AUTHORITY OF OFFICIALS REQUESTING PROTECTED HEALTH INFORMATION

Purpose

To ensure that Protected Health Information (PHI) is disclosed only to appropriate persons in accordance with the requirements of the HIPAA Privacy Rule.

Policy

It is the policy of this Facility to verify the identity and the authority of a person making a request for the disclosure of PHI, if the identity or authority of such person is not known to the Facility. Further, the Facility will obtain from the person seeking disclosure of PHI such documentation, statement or representation, as may be required by the HIPAA Privacy Rule, prior to a disclosure.

Procedure

1. In general, the Facility may rely on required documentation, statements or representations that, on their face, meet the verification requirements, if the reliance is reasonable under the circumstances. If there are concerns as to the requirements, contact the legal counsel.
2. Administrative Requests, Subpoena and Investigative Demand: Verification is sufficient and the Facility will disclose the requested PHI if the administrative document itself or a separate written statement recites:
 - a. The information sought is relevant to a lawful inquiry.
 - b. The request is specific and limited in scope, as much as practicable, for the purposes of the inquiry.
 - c. De-identified information could not be used.
3. Research: If disclosure is sought for research purposes, pursuant to a waiver of authorization, it is sufficient verification if the requesting documents:
 - a. Show that the waiver of authorization has been approved by a properly constituted Institutional Review Board or Privacy Board.
 - b. Is signed by the Chair of the Board or the Chair's Designee.
4. Requests by a Public Official
 - a. It is sufficient verification of the *identity* of the requesting person to rely on any of the following, if reasonable under the circumstances:
 - i. A badge or other credential
 - ii. A request on government letterhead.
 - iii. If the person making the request is acting on behalf of a public official, a written statement on government letterhead that the person is acting on behalf of a public official. If other authority is presented, contact legal

counsel for guidance before disclosure.

b. It is sufficient verification of the *authority* of the requesting person to rely on any of the following, if reasonable under the circumstances:

i. A written statement of the authority under which the information is requested, for example, a copy of the law or regulation. Rarely, a written statement is impractical, and then an oral statement is sufficient.

ii. Verification of authority is presumed if the request is made pursuant to a warrant, subpoena, order or other process issued by a grand jury, court or judge or administrative tribunal.

5. If the disclosure is sought by persons involved in the patient's care, and it is relevant to the requesting party's involvement in the care, the Facility may rely on reasonable professional judgment in verifying the identity and authority of the person seeking disclosure.

6. Verification requirements are met if the Facility, in good faith, makes a disclosure of PHI:

a. To prevent or lessen a serious and imminent threat to the health or safety of a person or the public, or

b. To law enforcement authorities to identify or apprehend an individual.

HIPAA DOCUMENTATION SECTION: **RETENTION OF PROTECTED HEALTH INFORMATION**

Purpose

To ensure appropriate retention of Protected Health Information (“PHI”) contained in a Designated Record Set.

Policy

PHI contained in the Designated Record Set will be retained according to state and federal regulations whichever requires retention for the longer period of time.

PHI, including medical and financial records contained in the Designated Record Set, will be retained for a minimum of six years as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule.

In absence of state law specifying a greater retention period, Medical Records must be retained for at least six years after the date it was last in effect.

For minor patients (persons who have not reached full legal age), the Medical Record must be retained for three years after the minor reaches legal age under state law or six years from the date of discharge, whichever is longer.

Medical records on which there may be pending litigation may be exempt from scheduled destruction at the discretion of the Facility.

If state laws and regulations require a greater retention time period, the greater will be followed.

Procedure

1. The Facility will review state laws and regulations to determine Medical Record retention period and “legal age.”
2. If state laws or regulations require a different retention period, the greater retention period will be followed.
3. The Facility will store the records until the retention period has expired. Records must be stored in a secure manner. The records must be protected from unauthorized access and accidental/wrong destruction.
4. At the expiration of the retention period, the Medical Records will be destroyed. Records should be destroyed annually in accordance with the retention time frames.

DESTRUCTION OF PROTECTED HEALTH INFORMATION

Purpose

To ensure that any medium containing Protected Health Information (“PHI”) is properly destroyed.

Policy

PHI stored in paper, electronic or other format will be destroyed utilizing an acceptable method of destruction after the appropriate retention period has been met.

Access to PHI stored on computer equipment and media will be limited by taking the appropriate measures to destroy electronically stored PHI.

Procedure

Paper Documents:

1. PHI maintained in paper format will be destroyed at the end of the retention period. (See the Policy “Retention of Protected Health Information.”)
2. All paper documents that contain PHI will be destroyed using an acceptable method of destruction.
3. Acceptable methods of destruction include shredding, incineration, pulverization and use of a bonded recycling company.
4. An *Inactive Medical Record Filing/Destruction Log* (“*Destruction Log*”) must be maintained to identify the destroyed records. At a minimum, the *Destruction Log* must capture the information listed below.
 - a. Date of destruction (date/s records are destroyed),
 - b. Destroyed by (name/s of the individuals responsible for destroying the records),
 - c. Witness (name/s of the person witnessing the destruction),
 - d. Method of destruction (method used to destroy records), and
 - e. patient information (full name, Medical Record number, date of admission, date of discharge).

(See sample *Destruction Log* following this Policy.)

5. Prior to destruction of boxed items, the Facility will verify the retention period has expired.
6. If the records are destroyed off-site through a destruction company, a Certificate of Destruction should be obtained attesting to destruction of the records.
7. The Facility will maintain destruction documents permanently.

Computer Data Storage Media

1. Personal Computers: Workstations, laptops and servers use hard drives to store a wide variety of information. patients' health information may be stored in a number of areas on a computer hard drive. For example, health information may be stored in "Folders" specifically designated for storage of this type of information, in temporary storage areas and in cache. Simply deleting the files or folders containing this information does not necessarily erase the data.
 - a. To ensure that any patients' health information has been removed, a utility that overwrites the entire disk drive with "1"s and "0"s must be used.
 - b. If the computer is being re-deployed internally or disposed of due to obsolescence, the aforementioned utility must be run against the computer's hard drive, after which the hard drive may be reformatted and a standard software image loaded on the reformatted drive.
 - c. If the computer is being disposed of due to damage and it is not possible to run the utility to overwrite the data, then the hard drive must be removed from the computer and physically destroyed. Alternatively, the drive can be erased by use of magnetic bulk eraser. This applies to PC workstations, laptops and servers.
2. Backup or Data Tapes:
 - a. Tapes are typically re-used many times but generally only by the data processing groups within the Facility, which routinely must handle patient health information. However, there may be situations where tapes are sent to external recipients for specific processing. Tapes used for this purpose should be segregated from the general pool used for backups. These tapes should be degaussed prior to use in creating the files being sent to ensure that no prior patient health information remains on that portion of the tape beyond the end of the current file.
 - b. Tapes or diskettes that are being decommissioned must be degaussed before disposal. This can be accomplished using a bulk tape eraser. Alternatively, the media may be pulverized or shredded.
3. Compact Disks (CDs) and Diskettes: CDs containing patient health information must be cut into pieces or pulverized before disposal.
4. If a service is used for disposal, the vendor should provide a certificate indicating the following:
 - a. Computers and media that were decommissioned have been disposed of in accordance with environmental regulations as computers and media may contain hazardous materials.
 - b. Data stored on the decommissioned computer and/or media was erased or destroyed per the previously stated method(s) prior to disposal.

Date of Destruction: _____

Witness: _____

Destroyed By: _____

Method of Destruction: _____

Center Name / Number: _____

HIM Representative: _____

The information described above was destroyed in the normal course of business pursuant to proper retention schedules as determined by Federal and State law and destruction policy and procedure.

Retain log permanently.

GLOSSARY

A

Accounting of Disclosures –

A log that is maintained for each patient that indicates the disclosures that have been made of his or her PHI.

Active Medical Record –

The active Medical Record consists of two parts: (1) the active record which is filed at the nurses' station/active record storage area and (2) the overflow files. (See also Medical Record.)

Administrative Tribunal –

A judge or group of judges who conduct hearings and exercise judgment over specific issues involving persons or things.

Administrative – connotes of or pertains to administration, especially management, as by managing or conducting, directing or superintending the execution, application, or conduct of persons or things.

Tribunal – is the seat of a judge; the place where he administers justice. The whole body of judges who compose a jurisdiction; a judicial court; the jurisdiction that the judges exercise.

Alternative Communication Means –

Information or communications delivered to patients by the Facility in a manner different than the normal practice of the Facility. For example, the patient may ask for delivery at an alternative address, phone number or post office box; or that discussion of PHI be limited when specified people are present.

Amend / Amendment –

An amendment to PHI will always be in the form of information *added to* the existing PHI. This additional information may contain items that substantially change the initial PHI, make parts of the initial PHI more precise, or show some of the original PHI to be incorrect. However, the original PHI is never altered. Changes are indicated by the addition of the amended information.

Authorization –

A patient's statement of agreement to the use or disclosure of Protected Health Information to a third party.

B

Business Associate (BA) –

A person or organization that performs a function or an activity on behalf of the Facility that involves the use or disclosure of Protected Health Information. A business associate might also be a person or entity that provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services involving the use or disclosure of PHI.

C

CMS – Centers for Medicare and Medicaid Services –

The agency formerly known as HCFA (Health Care Financing Administration) that regulates and enforces Federal Regulations for Medicare in Long Term Care and other health care entities.

Conditioned –

An authorization is “conditioned” if a patient cannot obtain treatment or service unless he or she signs that authorization.

Continuum of Care –

A range of services available to people in the community. They include supportive, rehabilitative, preventive and social services. They meet various levels of need or impairment.

Court Order –

An order issued from a competent court that requires a party to do or abstain from doing a specific act.

Covered Entity –

A health care provider who transmits health care information using one of the transaction standards defined by the Department of Health and Human Services. An example of this would be billing Medicare and Medicaid electronically for services your Facility provides to a patient.

D

De-Identification –

The process of converting individually identifiable information into information that no longer reveals the identity of the patient. Information may be de-identified by statistical de-identification or the safe harbor method of de-identification.

De-Identified Health Information –

Health information that does not identify an individual and does not contain information that can identify or link the information to the individual to whom the information belongs.

Department of Health and Human Services (HHS) –

The federal agency charged with the development, statement and implementation of the HIPAA Privacy Rule.

Designated Record Set –

patient Medical Records and billing records maintained and used by the Facility to make decisions about the patient. In this context a record is any item, collection, or grouping of information that contains Protected Health Information and is maintained, collected, used or disclosed by the Facility. The Designated Record Set also includes billing information that may contain ICD-9-CM codes that represent health conditions of the patient and that are part of the patient's Protected Health Information.

For access to the Designated Record Set, the State Operations Manual [SOM] (F153) allows the patient to "have access to all records pertaining to him or her including current clinical records." The Guidance to Surveyors indicates that the term "records" includes "all records pertaining to the patient such as trust fund ledgers pertinent to the patient and contracts between the patient and the Facility."

The SOM (F164) further defines personal records in the Guidance to Surveyors to include all types of records the Facility might keep on a patient, whether they are medical, social, fund accounts, automated or other.

Directory Information –

The four pieces of information that are considered "Directory Information" include:

- patient name
- Location in the Facility (room/bed number)
- Condition described in general terms (e.g., "He is not feeling well." or "She is having a good day.")
- Religious affiliation (available only to members of the clergy)

Note: You would not want to post or display more than the patient's name and room/bed number on your Facility directory.

Disclosure –

To release, transfer, provide access to or divulge in any way a patient's health information to individuals or entities outside your Facility. (See also Use.)

Routine Disclosure – Customary disclosures of PHI that the Facility discloses on a regular basis.

Non-Routine Disclosure – Disclosures of PHI that are not usually disclosed by the Facility.

E

F

Financial Records –

Admission, billing, and other financial information about a patient included as part of the Designated Record Set.

Fundraising –

An organized campaign by a private, non-profit or charitable organization designed to reach out to certain segments of the population or certain identified populations in an effort to raise monies for their organization or for a specific project or purpose espoused by their organization.

G

H

Health Care Operations –

Any of the following activities of a Facility:

1. Conducting quality assessment and improvement activities, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
2. Reviewing the competence or qualifications of health care professionals, evaluating employee and Facility performance, conducting training programs under supervision to practice or improve skills, training of non-health care professionals, accreditation, certification, licensing or credentialing activities;
3. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
4. Business planning and development such as conducting cost-management and planning related analyses related to managing and operating Facility;
5. Business management and general administrative activities of Facility/ campus, including, but not limited to:
 - Customer service
 - Resolution of internal grievances
 - Due diligence in connection with the sale or transfer of assets to a potential successor in interest
 - Creating de-identified health information, fundraising for the benefit of Facility/campus and

marketing for which an individual's authorization is not required.

Health Care Provider –

An entity that provides health care, service or supplies related to the health of an individual, e.g., medical, dental, physical therapy, or chiropractic clinics; hospitals, etc.

HIPAA –

Refers to the **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct of 1996, in particular the portion of the Act known as Administrative Simplification (Subpart F) dealing with the privacy of individually identifiable health information.

I

Individually Identifiable Health Information (IIHI) –

Any information, including demographic information, collected from an individual that:

1. Is created or received by a health care provider, health plan, employer or health care clearinghouse; and
2. Relates to the past, present or future physical or mental health or condition of an individual, and
 - a. Identifies the individual or
 - b. With respect to which there is reasonable basis to believe that the information can be used to identify the individual.

Institutional Review Board (IRB) –

In reference to a research project, a board that is designated to review and approve proposed research and the process by which the investigator intends to secure the informed authorization of participants.

L

Limited Data Set (LDS) –

A data set that includes elements such as dates of admission, discharge, birth and death as well as geographic information such as the five digit zip code and the individual's state, county, city or precinct but still excludes the other 16 elements that "de-identify" information. In addition, this limited data set can only be used if a covered entity enters into a "data use agreement" with the data recipient similar to the agreements entered into between covered entities and their business associates.

M

Marketing –

1. To provide information about a product or service that encourages recipients of the

communication to purchase or use the product or service, unless the communication is made:

- a. To describe a health-related product or service (or payment for such product or service) that is provided by or included in a plan of benefits of the covered entity making the communication, including communications about the entities participating in a health care provider network or health plan network; replacement of, or enhancement to, a health plan; and health-related products or services available only to a health plan enrollee that add values to, but are not part of, a plan of benefits;
 - b. For treatment of that individual; or
 - c. For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers or settings of care to the individual.
2. An arrangement between a covered entity and any other entity whereby the covered entity discloses Protected Health Information to the other entity in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

Medical Record: -

The collection of documents, notes, forms, test results, etc. which collectively document the health care services provided to an individual in any aspect of health care delivery by a provider; individually identifiable data collected and used in documenting healthcare services rendered. The Medical Record includes records of care used by healthcare professionals while providing patient care services, for reviewing patient data, or documenting observations actions or instructions. The Medical Record is included as part of the Designated Record Set.

Minimum Necessary –

The least amount of Protected Health Information needed to achieve the intended purpose of the use or disclosure. Covered Entities are required to limit the amount of Protected Health Information it uses, discloses or requests to the minimum necessary to do the job.

N

Notice of Privacy Practices –

A document required by HIPAA that provides the patient with information on how the Facility generally uses a patient's Protected Health Information and what the patient's rights are under the Privacy Rule.

O

Office of Civil Rights –

The agency with the U.S. Department of Health and Human Services that has responsibility for enforcement of the HIPAA Privacy Rule. (www.usda.gov/cr/)

Opt Out –

To make a choice to be excluded from services, procedures or practices. patient rights under HIPAA include many situations where the patient may request to be excluded from a service, procedure or practice. In most cases, the Facility must comply or attempt to comply with the request to be excluded.

P

Payment –

The activities undertaken by a health care provider or payer to obtain reimbursement for the provision of health care.

Patient –

As used in this Manual includes patient, the person receiving health care services.

Personal Representative –

Is the term used in the Privacy Rule to indicate the person who has authority under law to act on behalf of a patient. *For purposes of the Privacy Rule a Facility must treat a personal representative as having the same rights as the patient unless there is a reasonable belief that the personal representative has subjected the patient to abuse or neglect, or treating the person as the personal representative could endanger the patient.*

Policy –

A high-level over-all plan embracing the general principles and aims of an organization.

Pre-emption / Pre-empts –

Taking priority over or supercedes.

Privacy Breach –

A violation of one's responsibility to follow privacy policy and procedure that results in the patients' PHI being accessed by unauthorized persons.

Privacy Official –

The person in the Facility who is the designated point of contact for HIPAA-related issues and whose position includes oversight of training related to HIPAA. May also be called the Privacy Representative or the HIPAA Point of Contact (HPOC).

Privacy Officer –

The person designated by the organization who is responsible for development and implementation of the HIPAA policies and procedures. The Privacy Officer serves as a resource to assist each Facility's Privacy Official in implementing HIPAA policies and procedures. HIPAA requires that each covered

entity appoint a Privacy Official

Privacy Rule –

Refers to the regulation issued by the Department of Health and Human Services entitled Standards for Privacy of Individually Identifiable Health Information that was published on December 28, 2000, and subsequently modified on August 14, 2002. The effective date for the Privacy Rule is April 14, 2003. In this Policy and Procedure Manual, “HIPAA” and “Privacy Rule” are used interchangeably.

Protected Health Information (PHI) –

Information that is a subset of health information, including demographic information, and:

1. Is created or received by a health-care provider, health plan, employer or health-care clearinghouse; and
2. Relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and
 - a. That identifies the individual; or
 - b. There is a reasonable basis to believe the information can be used to identify the individual.

Psychotherapy Notes –

Notes that are recorded (in any medium) by a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint or family counseling session. Psychotherapy notes must be kept separate from the rest of the patient’s Medical Record.

Q

Qualified Protective Order –

A legal command intended to protect a person or thing from an unfair or unjust action.

Order – a mandate, precept; a command or direction authoritatively given; a rule or regulation.

R

Re-Identification –

The process of converting de-identified health information back to individually identifiable health information. Re-identified health information does reveal the identity of the patient and must be treated as PHI under the HIPAA Privacy Rule.

Research –

A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalized knowledge.

Revoke –

To cancel or withdraw an authorization to release medical information.

Role Based Access –

Access to PHI based on the duties of employees. The Facility will identify persons or classes of persons in its workforce who need access to PHI to carry out their duties and make a reasonable effort to limit access PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

S

Safeguarding –

To ensure safekeeping of Protected Health Information for the patient.

Security Officer –

A position mandated by the HIPAA. The responsibilities of this person are to oversee implementation of the requirements mandated by the Final Security regulation and any security requirements included in the other sections of the HIPAA regulation.

State Operations Manual (SOM) –

Federal Regulations that govern all Skilled Nursing Facilities that receive federal funding from Medicare and/or Medicaid.

Subpoena (2 Kinds) –

A process to cause a witness to appear and give testimony, commanding him to lay aside all pretenses and excuses, and appear before a court or magistrate therein named at a time therein mentioned to testify for the party named under a penalty thereof.

Duces Tecum –A request for witnesses to appear and bring specified documents and other tangible items. The subpoena *duces tecum* requires the individual to appear in court with the requested documents, or simply turn over those documents to the court or to counsel requesting the documents.

General Subpoena (AKA Ad Testificandum) –A command to appear in court at a certain time and place to give testimony regarding a certain matter, for example, to testify that the record was kept in the normal course of business.

T

TPO –

(See Treatment, Payment and Operation.)

Treatment –

The provision, coordination or management of health care and related services by the Facility, including the coordination or management of health care by the Facility with a third party; consultation with other health care providers relating to a patient; or the referral of a patient for health care between the Facility and another health care provider.

Treatment, Payment and Operations (TPO) –

The Privacy Rule allows sharing of information for purposes of treatment, payment and health care operations. Treatment includes use of patient information for providing continuing care. Payment includes sharing of information in order to bill for the care of the patient. Health care operations are certain administrative, financial, legal, and quality improvement activities that are necessary for your Facility to run its business and to support the core functions of treatment and payment.

U

Use –

To share, apply, use, examine or analyze health information within the Facility. (See also Disclosure).

V

W

Whistleblower –

A person, usually a staff member, who reveals wrongdoing within an organization to the public, government agencies or to those in positions of authority.

Workforce –

Employees, volunteers, trainees and other persons whose conduct, in the performance of work for the Facility, is under the direct control of the Facility, whether or not they are paid. Members of the workforce are not business associates.