

DRAFT

If you choose to use these or any other sample forms, agreements or policies, you must review them with your attorney before implementing them.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is distributed with the understanding that the Eastern PA EMS Council is ***not*** engaged in rendering any legal or professional services. If legal advise or other expert assistance is required, the services of a competent professional person should be sought.

Draft
Terms

Business Associate (BA): A person or organization that performs an activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, and company management, on behalf of a covered entity, but is not part of the covered entity's workforce. A business associate can also be a covered entity in its own right.

Covered Entity (CE): Under HIPAA, this is a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a HIPAA transaction.

Designated Record Set

A group of records maintained by or for a covered entity that is:

- a. The medical records and billing records about individuals maintained by or for a covered health care provider;
- b. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
- c. Used, in whole or in part, by or for the covered entity to make decisions about individuals.

Health Information: any information, whether oral or recorded in any form or medium, that

- a. is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse, and
- b. 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 provision of health care to an individual.

Health Insurance Portability and Accountability Act of 1996 (HIPAA): A Federal law that allows persons to qualify immediately for comparable health insurance coverage when they change their employment relationships. Title II, Subtitle F, of HIPAA gives HHS the authority to mandate the use of standards for the electronic exchange of health care data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for health care patients, providers, payers (or plans), and employers (or sponsors); and to specify the types of measures required to protect the security and privacy of personally identifiable health care information. Also known as the Kennedy-Kassebaum Bill, the Kassebaum-Kennedy Bill, K2, or Public Law 104-191. Accountability Act of 1996.

Individually identifiable data is data that can be readily associated with a specific individual. Examples would be a name, a personal identifier, or a full street address. If life was simple, everything else would be non-identifiable data. But even if you remove the obviously identifiable data from a record, other data elements present can also be used to re-identify it. For example, a birth date and a zip code might be sufficient to re-identify half the records in a file. The re-identifiability of data can be limited by omitting, aggregating, or altering such data to the extent that the risk of it being re-identified is acceptable.

Draft

Individually Identifiable Health Information (IIHI) and Protected Health Information (PHI)

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

- (1) Is created or received by a health care provider,
- (2) relates to past, present or future health condition, provision of health care or payment for health care; and
 - a. That identifies the individual; or
 - b. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Protected health information means individually identifiable health information with a few statutory exemptions.

Marketing: Marketing means to make a communication about a product or service a purpose of which is to encourage recipients of the communication to purchase or use the product or service.

Marketing does not include:

- (i) describing the entities participating in a health care provider network or health plan network, or for the purpose of describing if and the extent to which a product or service (or payment for such product or service) is provided by a covered entity or included in a plan of benefits; or
- (ii) communication made by health care provider as part of treatment or to further treatment or to recommend alternative treatments, health care providers, therapies or settings for care
- (iii) the communication is made orally
- (iv) the communication is in writing and the covered entity does not receive direct or indirect remuneration from a third party for making the communication.

Minimum Scope of Disclosure or “Minimum Necessary”: The principle that, to the extent practical, individually identifiable health information should only be disclosed to the extent needed to support the purpose of the disclosure.

Treatment, Payment and Health Care Operations

Treatment includes consultation, referral, coordination and management of care

Payment - activities of provider to obtain reimbursement, including: determinations of eligibility, billing, utilization review, and disclosure relating to collections

Health Care Operations – include any of the following:

- (i) Quality assessment and improvement
- (ii) Credentialing activities and education and training programs
- (iii) Arranging for medical review, legal services, auditing
- (iv) Business planning and development
- (v) Business management and administration

Draft

IDENTIFY PRIVACY OFFICIAL AND CONTACT PERSON, POLICY

General Requirements:

A covered entity must designate a privacy official who will be responsible for the development and implementation of the policies and procedures that comply with the HIPAA regulations.

A covered entity must also designate a contact person or office that is responsible for:

- receiving complaints concerning the substance of the provider's HIPAA policies and procedures
- receiving complaints concerning the covered entity's compliance with such policies and procedures or with the requirements of the HIPAA Privacy Rule generally; and
- providing further information about matters covered by the notice of privacy required by 164.520 of the HIPAA Privacy Rule

Policies and Procedures:

A written or electronic record of the designation of the privacy official and the contact person/office must be maintained.

Identity of Contact Person:

The contact person may be, but is not required to be, the same individual as the privacy official. The choice in that regard is left to the discretion of the covered entity.

If you use the model policies,
agreements and forms here, you must
have them reviewed by your attorney
before implementing them.

You must review the policies, agreements and forms and revise them for use by your organization.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is distributed with the understanding that the Eastern PA EMS Council is ***not*** engaged in rendering any legal or professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

Draft

NOTICE OF PRIVACY, MODEL FORM

[Company Name]

Notice of Privacy As required by the Privacy Regulations created as a result of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

THIS NOTICE DESCRIBES HOW HEALTH INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED, AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.

PLEASE REVIEW THIS NOTICE CAREFULLY.

If you have any questions about this notice please contact our privacy contact who is [insert name, address and phone number of contact]

This Notice of Privacy describes how our company may use and disclose your protected health information to carry out treatment, payment or health care operations and for other purposes that are permitted or required by law. It also describes your rights to access and control your protected health information. "Protected health information" (PHI) is information about you, including demographic information, that may identify you and that relates to your past, present or future physical or mental health or condition and related health care services. Our Company is dedicated to maintaining the privacy of your protected health information.

We are required to abide by the terms of this Notice of Privacy. We may revise or amend the terms of our notice, at any time. The new notice will be effective for all protected health information that we have at that time and for future information. We will post our current Notice in our office in a visible location at all times and upon your request, we will provide you with any revised Notice.

DISCLOSURES

Uses and Disclosures to carry out treatment, payment or health care operations:

Under HIPAA regulations, we do not need to obtain permission to use health information for treatment, payment and health care operations.

We may use and disclose your Protected Health Information (PHI) for the following reasons:

Treatment: We will use and disclose your PHI to provide, coordinate, or manage your health care and any related services. This includes the coordination or management of your health care with a third party.

We may disclose your PHI to others who may assist in your care, such as your spouse, children or parents. Finally, we may also disclose your PHI to other health care providers for purposes related to your treatment.

Payment: Your protected health information will be used, as needed, to obtain payment for your health care services. This may include certain activities that your health insurance plan may undertake before it approves or pays for the health care services we provided for you.

Healthcare Operations: We may use or disclose, as-needed, your protected health information in order to support the business activities of (company name). These activities include, but are not limited to, quality assessment activities, employee review activities, training of students, certification activities.

Draft

We will share your protected health information with third party “business associates” that perform activities (e.g., billing) for the company. However, whenever an arrangement between our office and a business associate involves the use or disclosure of your protected health information, we will have a written contract that contains terms that will protect the privacy of your protected health information.

Appointment Reminders (if applicable) We may use or disclose your protected health information, as necessary, to contact you to remind you of appointments or prescheduled transports.

Treatment Options and Services (if applicable) We may use or disclose your protected health information, as necessary, to provide you with information about transport alternatives or other health-related benefits and services that may be of interest to you. However, we will get a written authorization from you for further marketing purposes.

2. Uses and disclosures that you can agree or object to

We may use and disclose your protected health information in the following instances, which you have the opportunity to object to.

Others Involved in Your Healthcare: Unless you object, we may disclose to a member of your family, a relative, a close friend or any other person you identify, your protected health information that directly relates to that person’s involvement in your health care. If you are unable to agree or object to such a disclosure, we may disclose such information as necessary if we determine that it is in your best interest based on our professional judgment. We may use or disclose protected health information to notify or assist in notifying a family member, personal representative or any other person that is responsible for your care of your location, general condition or death. Finally, we may use or disclose your protected health information to an authorized public or private entity to assist in disaster relief efforts and to coordinate uses and disclosures to family or other individuals involved in your health care.

Emergencies We may use or disclose your protected health information in an emergency treatment situation. If this happens, your physician shall allow you to object to future disclosures as soon as reasonably practicable after the delivery of treatment.

3. Uses and disclosures that we will obtain your written authorization for

Marketing for most marketing purposes we will obtain your written consent.

4. Uses and disclosures for which an authorization or opportunity to agree or object to is not required

We may use or disclose your protected health information in the following situations:

Required By Law: We may use or disclose your protected health information to the extent that the use or disclosure is required by law. The use or disclosure will be made in compliance with the law and will be limited to the relevant requirements of the law. You will be notified, as required by law, of any such uses or disclosures.

Public Health: We may disclose your protected health information for public health activities and purposes to a public health authority that is required or permitted by law to receive the information. The disclosure will be made for the purpose of controlling or reporting disease, injury or disability. We may also disclose your protected health information, if directed by the

Draft

public health authority, to a foreign government agency that is collaborating with the public health authority.

Communicable Diseases: We may disclose your protected health information, if authorized by law, to a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading the disease or condition.

Abuse or Neglect: We may disclose your protected health information to a public health authority that is authorized by law to receive reports of child abuse or neglect. In addition, we may disclose your protected health information if we believe that you have been a victim of abuse, neglect or domestic violence to the governmental entity or agency authorized to receive such information. In this case, the disclosure will be made consistent with the requirements of applicable federal and state laws.

Maintenance of Vital Records: We may report data such as births and deaths.

Health Oversight: We may disclose protected health information to a health oversight agency for activities authorized by law, such as audits, investigations, and inspections. Oversight agencies seeking this information include government agencies that oversee the health care system, government benefit programs, other government regulatory programs and civil rights laws.

Legal Proceedings: We may disclose protected health information in the course of any judicial or administrative proceeding, in response to an order of a court or administrative tribunal (to the extent such disclosure is expressly authorized), in certain conditions in response to a subpoena, discovery request or other lawful process.

Law Enforcement: We may also disclose protected health information, so long as applicable legal requirements are met, for law enforcement purposes. These law enforcement purposes include (1) legal processes and otherwise required by law, (2) limited information requests for identification and location purposes, (3) pertaining to victims of a crime, (4) suspicion that death has occurred as a result of criminal conduct, (5) in the event that a crime occurs on the premises of the company and (6) medical emergency (not on the company's premises) and it is likely that a crime has occurred.

Coroners, Funeral Directors, and Organ Donation: We may disclose protected health information to a coroner or medical examiner for identification purposes, determining cause of death or for the coroner or medical examiner to perform other duties authorized by law. We may also disclose protected health information to a funeral director, as authorized by law, in order to permit the funeral director to carry out their duties. We may disclose such information in reasonable anticipation of death. Protected health information may be used and disclosed for cadaveric organ, eye or tissue donation purposes.

Research: We may disclose your protected health information to researchers when their research has been approved by an institutional review board that has reviewed the research proposal and established protocols to ensure the privacy of your protected health information. Otherwise, we will ask for a written authorization from you.

Criminal Activity: Consistent with applicable federal and state laws, we may disclose your protected health information, if we believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. We may also disclose protected health information if it is necessary for law enforcement authorities to identify or apprehend an individual.

Draft

Workers' Compensation: Your protected health information may be disclosed by us as authorized to comply with workers' compensation laws and other similar legally-established programs.

Required Uses and Disclosures: Under the law, we must make disclosures to you and when required by the Secretary of the Department of Health and Human Services to investigate or determine our compliance with the requirements of Section 164.500 et. seq.

YOUR RIGHTS

Following is a statement of your rights with respect to your protected health information and a brief description of how you may exercise these rights.

You have the right to inspect and copy your protected health information. This means you may inspect and obtain a copy of protected health information about you that is contained in a designated record set for as long as we maintain the protected health information. A "designated record set" contains medical and billing records and any other records that your physician and the Company uses for making decisions about you. This may not include psychotherapy notes.

You must submit your request in writing to [insert name, or title, and telephone number of a person or office to contact for further information] in order to inspect and/or obtain a copy of your PHI. Our Company may charge a fee for the costs of copying, mailing, labor and supplies associated with your request. Our Company may deny your request to inspect and/or copy in certain limited circumstances; however, you may request a review of our denial. Another licensed health care professional chosen by us will conduct reviews.

Please contact [name, title and telephone number] if you have questions about access to your medical record.

You have the right to request a restriction of your protected health information. This means you may ask us not to use or disclose any part of your protected health information for the purposes of treatment, payment or healthcare operations. You may also request that any part of your protected health information not be disclosed to family members or friends who may be involved in your care or for notification purposes as described in this Notice of Privacy. Your request must state the specific restriction requested and to whom you want the restriction to apply. Your physician is not required to agree to a restriction that you may request.. You may request a restriction by **contacting:**

Privacy Officer

Address, phone

You have the right to request that our Company communicate with you about your health and related issues in a particular manner or at a certain location. For instance, you may ask that we contact you at home, rather than work. In order to request a type of confidential communication, you must make a written request to [insert name, or title, and telephone number of a person or office to contact for further information] specifying the requested method of contact, or the location where you wish to be contacted. Our Company will accommodate reasonable requests. You do not need to give a reason for your request.

Draft

You may have the right to have the company amend your protected health information. This means you may request an amendment of protected health information about you in a designated record set for as long as we maintain this information. In certain cases, for example if we think the information is correct, or was not created by our Company, we may deny your request for an amendment. If we deny your request for amendment, you have the right to file a statement of disagreement with us and we may prepare a rebuttal to your statement and will provide you with a copy of any such rebuttal. Please contact our Privacy Contact to determine if you have questions about amending your medical record. To file an amendment, your request must be in writing and must be submitted to [insert name, or title, and telephone number of a person or office to contact].

You have the right to receive an accounting of certain disclosures we have made, if any, of your protected health information. This right applies to disclosures for purposes other than treatment, payment or healthcare operations as described in this Notice of Privacy Statement. Accounting is not required for disclosures we may have made to you, incidental disclosures, disclosures you have authorized, disclosures for a facility directory, disclosures to family members or friends involved in your care, or disclosures made to carry out treatment, payment or health care operations. You have the right to receive specific information regarding disclosures that occurred after April 14, 2003 up to a six year timeframe. You may request a shorter timeframe. The right to receive this information is subject to certain exceptions, restrictions and limitations.

In order to obtain an accounting of disclosures, you must submit your request in writing to [insert name, or title, and telephone number of a person or office to contact for further information]. The Company may charge you for additional lists within the same 12-month period. Our Company will notify you of the costs involved with additional requests, and you may withdraw your request before you incur any costs.

You have a right to a paper copy of this notice. You are entitled to receive a paper copy of our notice of privacy even if you have agreed to receive an electronic copy of the Notice. You may ask us to give you a copy of this notice at any time. To obtain a paper copy of this notice, contact [insert name, or title, and telephone number of a person or office to contact for further information].

You have a right to file a complaint if you believe your privacy rights have been violated. You may file a complaint with our Company or with the Secretary of the Department of Health and Human Services. To file a complaint with our Company, contact [insert the name, title, and phone number of the contact person or office responsible for handling complaints]. All complaints must be submitted in writing. You will not be penalized for filing a complaint.

This notice was published and becomes effective on [complete with a date which should be no later than April 14, 2003.]

Draft

MODEL ACKNOWLEDGEMENT OF RECEIPT OF NOTICE FORM

COMPANY NAME

ACKNOWLEDGEMENT OF RECEIPT OF NOTICE OF PRIVACY

I, _____, have received a copy of _____'s Notice
Patient Name Company Name
of Privacy Practices Policy.

Signature of Patient

Date

Draft

(Company)

Consent for Purposes of Treatment, Payment and Healthcare Operations

I consent to the use or disclosure of my protected health information by [Company Name] for the purpose of diagnosing or providing treatment to me, obtaining payment for my health care bills or to conduct health care operations of [Company Name].

I have the right to revoke this consent, in writing, at any time, except to the extent that [Company Name] has taken action in reliance on this consent.

My "protected health information" means health information, including my demographic information, collected from me and created or received by my physician, another health care provider, a health plan, my employer or a health care clearinghouse. This protected health information relates to my past, present or future physical or mental health or condition and identifies me, or there is a reasonable basis to believe the information may identify me.

Signature of Patient or Personal Representative

Name of Patient or Personal Representative

Date

Description of Personal Representative's Authority

BUSINESS ASSOCIATE AGREEMENT

(Intended to be an Amendment or Addendum to an Agreement
For Services Involving the Use, Creation or Transmission of
Protected Health Information)

This Business Associate Agreement (“Agreement”) effective on _____, 2002 (“Effective Date”) is entered into by and between _____ (the “Business Associate”) and _____ (the “Covered Entity”).

A. The purpose of this Agreement is to comply with the Standards for Privacy of Individually Identifiable Health Information (“protected health information”) published on August 14, 2002 by the Secretary of the U.S. Department of Health and Human Services (“HHS”) to amend 45 C.F.R. Part 160 and Part 164 (the “Privacy Regulation”) under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”).

B. [Covered Entity has requested Business Associate to perform the services set forth in Attachment A hereto with the condition that Business Associate agrees to abide by the requirements set forth in the Privacy Regulation.]

C. This Agreement sets forth the terms and conditions pursuant to which protected health information that is provided by, or created or received by, the Business Associate from, or on behalf of, the Covered Entity will be handled.

In consideration of the previous statements and agreements hereinafter addressed, the parties agree as follows:

1. Services. The Business Associate provides services for the Covered Entity that involve the use and disclosure of protected health information which services are described in Attachment A hereto. Except as otherwise specified herein, the Business Associate may make any and all uses of protected health information necessary to perform its obligations as set forth in Attachment A and/or under the Services Agreement between the parties. Additionally, Business Associate may disclose protected health information for the purposes authorized by this Agreement only (a) to its employees, subcontractors and agents, in accordance with Section 2(d), or (b) as directed by the Covered Entity.
2. Responsibilities of Business Associate. With regard to its use and/or disclosure of protected health information, the Business Associate hereby agrees to do the following:
 - (a) Use and/or disclose the protected health information only as permitted or required by this Agreement or as otherwise required by law;
 - (b) Report to the designated privacy officer of the Covered Entity, in writing, any use and/or disclosure of the protected health information that is not permitted or required by this Agreement of which Business Associate becomes aware within fifteen (15) days of the Business Associate’s discovery of such unauthorized use and/or disclosure;

Draft

(c) Use commercially reasonable efforts to maintain the security of the protected health information and to prevent unauthorized use and/or disclosure of such protected health information;

(d) Require all of its employees, representatives, subcontractors or agents that receive or use or have access to protected health information under this Agreement to agree in writing to adhere to the same restrictions and conditions on the use and/or disclosure of protected health information that apply herein, including the obligation to return or destroy the protected health information as provided under (h) of this section.

(e) Make available all records, books, agreements, policies and procedures relating to the use and/or disclosure of protected health information to the Secretary of HHS for purposes of determining the Covered Entity's compliance with the Privacy Regulation, subject to attorney-client and other applicable legal privileges.

(f) Upon written request, make available during normal business hours at Business Associate's offices all records, books, agreements, policies and procedures relating to the use and/or disclosure of protected health information to the Covered Entity within (____) days for purposes of enabling the Covered Entity to determine the Business Associate's compliance with the terms of this Agreement;

(g) Within forty five (45) days of receiving a written request from the Covered Entity, provide to the Covered Entity such information as is requested by the Covered Entity to permit the Covered Entity to respond to a request by the subject individual for amendment and accounting purposes of the disclosures of the individual's protected health information in accordance with 45 C.F.R. §164.526 and §164.528;

(h) Return to the Covered Entity or destroy, as requested by the Covered Entity, within ____ (__) days of the termination of this Agreement, the protected health information in Business Associate's possession and retain no copies or back-up tapes; and

(i) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of protected health information by Business Associate in violation of the requirements of this Agreement.

3. Responsibilities of the Covered Entity. With regard to the use and/or disclosure of protected health information by the Business Associate, the Covered Entity hereby agrees:

(a) To inform the Business Associate of any changes in the form of notice of privacy that the Covered Entity provides to individuals pursuant to 45 C.F.R. §164.520 and provide the Business Associate a copy of the notice currently in use;

(b) To inform the Business Associate of any changes in, or withdrawal of, the consent or authorization provided to the Covered Entity by individuals whose protected health information may be used and/or disclosed by Business Associate under this Agreement pursuant to 45 C.F.R. §164.506 or §164.508; and

(c) To notify the Business Associate, in writing and in a timely manner, of any restrictions on the use and/or disclosure of protected health information agreed to by the Covered Entity as provided for in 45 C.F.R. §164.522.

4. Mutual Representation and Warranty. Each party represents and warrants to the other party that all of its employees, agents, representatives and members of its work force, who services may be used to fulfill obligations under this Agreement, are or shall be appropriately informed of the terms of this Agreement and are under legal obligation to fully comply with all provisions of this Agreement.

5. Term and Termination.

(a) Term. This Agreement shall become effective on the Effective Date and shall continue in effect until all obligations of the parties have been met, unless terminated as provided herein or by mutual agreement of the parties.

(b) Termination. As provided for under 45 C.F.R. §164.504(e)(2)(iii), the Covered Entity may immediately terminate this Agreement and any related agreement if it determines that the Business Associate has breached a material provision of this Agreement. Alternatively, the Covered Entity may choose to: (i) provide the Business Associate with ____ (__) days written notice of the existence of an alleged material breach; and (ii) afford the Business Associate an opportunity to cure said alleged material breach upon mutually agreeable terms. Failure to cure in the manner set forth in this paragraph is grounds for the immediate termination of the Agreement. If termination is not feasible, the Covered Entity shall report the breach to the Secretary of HHS. This Agreement will automatically terminate without any further action of the parties upon the termination or expiration of the Service Agreement between the parties.

(c) Effect of Termination. Upon termination of this Agreement, for any reason, Business Associate shall return or destroy all protected health information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the protected health information.

6. Survival. The respective rights and obligations of Business Associate and Covered Entity under the provisions of Sections 2(h) and 2(i) and 8 shall survive the termination of this Agreement indefinitely.

7. Amendment. This Agreement may not be modified or amended, except in writing as agreed to by each party. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.

Draft

8. Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule.

IN WITNESS WHEREOF, the parties hereto hereby set their hands and seals as of the ____ day of _____, 2002.

IN PRESENCE OF:

Business Associate

Witness

By: _____
Name: _____
Title: _____
Date: _____

Witness

Company

By: _____
Name: _____
Title: _____
Date: _____

(company)
Staff Confidentiality Agreement

It is imperative that our personnel maintain the confidentiality of patient information that we receive in the course of our operations. (company) expressly prohibits the release of any patient information to anyone outside the organization unless required for purposes of treatment, payment, or health care operations. Discussions of Protected Health Information (PHI) within the organization should be limited to acceptable uses only. Acceptable uses of PHI include, but are not limited to, exchange of patient information required for the treatment of the patient, billing, and other health care operations, peer review, internal audits, and quality assessment and improvement activities.

I understand that (company) provides services to patients that are private and confidential and that I occupy an important part in maintaining the privacy rights of (company)'s patients. I understand that it is necessary, in the rendering of (company) services, that patients provide personal information in the form of electronic, oral, written or photographic media and that this information is strictly confidential and protected by federal and state laws.

I agree that I will comply with all confidentiality policies, practices and procedures instituted by _____ (company) during my entire employment or association with _____ (company). If I, at any time, knowingly or inadvertently, violate the patient confidentiality policies, practices and procedures, I agree to notify the Privacy Officer of _____ (company) immediately. I understand that a violation of patient confidentiality may result in the suspension or termination of my employment or association with _____ (company). Upon termination of my employment or association for any reason, or at any time upon request, I agree to return any and all patient confidential information in my possession. This does not constitute a contract for continued employment.

I have read, and I understand all privacy policies and procedures that have been provided to me by _____ (company). I agree to obey all policies and practices or be subject to disciplinary action, which may include verbal or written warning, suspension, or termination of employment or membership or association with _____ (company). This is not a contract of employment and does not alter the nature of the existing relationship between _____ (company) and me.

Signature: _____ Date: _____

Printed Name: _____

Draft

Policy on Security, Levels of Access and Limiting Disclosure and Use of PHI Purpose

To outline levels of access to Protected Health Information (PHI) of various staff members of (company) and to provide a policy and procedure on limiting access, disclosure, and use of PHI. Security of PHI is everyone's Policy responsibility.

(Company) maintains strict requirements on the security, access, disclosure and use of PHI. Access, disclosure and use of PHI will be role based, and limited to the extent that the person needs access to PHI to complete necessary job functions.

When PHI is accessed, disclosed and used, the individuals involved will make every effort, except in patient care situations, to only access, disclose and use PHI to the extent that only the minimum necessary information is used to accomplish the intended purpose.

Procedure

Role Based or "need to know" Access

Access to PHI will be limited to those who need access to PHI to carry out their duties. The following describes the specific categories or types of PHI to which these persons need access is defined and the conditions, as appropriate, that would apply to such access.

Access to PHI is limited to the persons identified below only, and to the identified PHI only, based on (company's) determination of the persons or job descriptions of persons who require PHI, and the nature of the health information they require, consistent with the responsibilities of their position.

Access to a patient's entire file will not be allowed except when provided for in this and other policies and procedures and the justification for use of the entire medical record is specifically identified and documented.

EMT	Patient Care reports	as part of completion of duties And only while on duty
Paramedic	Patient Care reports	as part of completion of duties and Only while on duty
Billing Clerk	Patient care reports, Claim forms, patient Care forms from facilities	as part of duties during work hours

Other positions as defined by your organization.

Disclosures to and Authorizations From the Patient

You are not required to limit to the minimum amount of information necessary required to perform your job function, or your disclosures of PHI to patients who are the subject of the PHI. In addition, disclosures authorized by the patient are exempt from the minimum necessary requirements unless the authorization to disclose PHI is requested by (Company)

Authorizations received directly from third parties, such as Medicare, or other insurance companies, which direct you to release PHI to those entities, are not subject to the minimum necessary standards.

Draft

For example, if we have a patient's authorization to disclose PHI to Medicare, Medicaid or another health insurance plan for claim determination purposes, (Company) is permitted to disclose the PHI requested without making any minimum necessary determination.

Company Requests for PHI

If (Company) needs to request PHI from another health care provider on a routine or recurring basis, we must limit our requests to only the necessary information needed for the intended purpose, as described below. For requests not covered below, you must make this determination individually for each request and you should consult your supervisor for guidance. For example, if the request is not routine, like requesting documents via a subpoena, we will make sure our request covers only the minimum necessary PHI to fulfill request. For all other requests, determine what information is reasonably necessary for each on an individual basis.

Examples:

A skilled nursing home may have records that we need for determine medical necessity and to bill for the service. You would request patient "face sheets", physician certifications and/or mobility assessments.

A mutual aid ambulance or paramedic service has records the service needs to conduct joint billing operations for mutually treated patients. You would request copies of patient care reports.

Incidental Disclosures

(Company) understands that there will be times when there are incidental disclosures about PHI during the care of a patient. The privacy laws were not intended to impede common health care practices that are essential in providing health care to the individual. Incidental disclosures are inevitable, but these will typically occur in radio or face-to-face conversation between health care providers, or when patient care information in written or computer form is left out in the open for others to access or see.

All staff must be aware of the importance of maintaining the confidence and security of all materials that we create or use containing patient care information. Personnel should not have access to information that is not necessary for him or her to complete his or her job.

All personnel must endeavor to avoid incidental disclosures to other health care providers and others who do not have a need to know the information. Pay attention to who is within audible range when you make verbal statements about a patient's health information, and use common sense procedures for avoiding accidental or inadvertent disclosures:

Verbal Security

Waiting or Public Areas: If patients are in waiting areas in your building to discuss the service provided to them or billing questions, ensure that there are no other persons in the waiting area. If other personnel are within audible range, take the patient into a more secure area to conduct the conversation.

Garage Areas: Staff members should be aware of the fact that members of the public and other agencies may be present in the building. Conversations about patients and their health care should not take place in areas where those who do not have a "need to know" are present.

Draft

Other Areas: Staff members should only discuss patient care information with those who are involved in the care of the patient, regardless of your physical location. Be aware of your level of voice and of the fact that others may be in the area when you are speaking. However, when it comes to treatment of the patient, you should be free to discuss all aspects of the patient's medical condition, treatment provided, and any of their health information you may have in your possession with others involved in the care of the patient.

Physical Security

Patient Care and Other Patient or Billing Records: Patient care reports must be stored in safe and secure areas. When any paper records concerning a patient are completed, they must be placed _____, not left in open bins or on desktops or other surfaces. Only those with a need to have the information for the completion of their job duties should have access to any paper records.

Billing records, including all notes, remittance advices, charge slips or claim forms should not be left out in the open and should be stored in files or boxes that are secure and in an area with access limited to those who need access to the information for the completion of their job duties.

Computers and Entry Devices: Computer access terminals and other remote entry devices such as PDAs and laptops should be kept secure. Access to any computer device should be by password only. Staff members should be aware of who may be able to see the monitor screen and take simple steps to shield the screen by unauthorized persons. All remote devices such as laptops and PDAs should remain in the physical possession of the individual to whom it is assigned at all times.

Draft

Company
Policy on Privacy Training

Purpose

To ensure that all members of (Company) staff, including all employees, volunteers, students and trainees, board of directors (collectively referred to as “staff members”) having access to patient information understand the organization’s concern for the respect of patient privacy and have been trained in the company’s policies and procedures regarding Protected Health Information (PHI).

Policy

1. All current staff, including Board of Directors, will be required to undergo privacy training in accordance with the HIPAA Privacy Rule prior to April 14, 2003.
2. All new staff members will be required to undergo privacy training in accordance with the HIPAA Privacy Rule within a reasonable time upon association with the organization. .
3. All staff members will be required to undergo privacy training in accordance with the HIPAA Privacy Rule within a reasonable time if there is a change to the Company’s privacy practices, policies or procedures .

Procedure

1. The Privacy Training will be conducted by the Privacy Officer or his or her designee.
2. All attendees will receive copies of the Company’s privacy practices, policies and procedures
3. All attendees must attend the training in person and verify his or her attendance.
4. All attendees must agree to adhere to the Company’s privacy practices, policies and procedures.
5. Training will be conducted by viewing a video or computer based program or by didactic presentation by the privacy officer or his or her designee.
6. Topics of the training will include a complete review of the Company’s Policy on Privacy Practices and will include other information concerning the HIPAA Privacy Rule, which may be the following topic areas:
 - a. Overview of the federal and state laws concerning patient privacy including the Privacy Regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
 - b. Description of protected health information (PHI)
 - c. Patient rights under the HIPAA Privacy Rule
 - d. Staff member responsibilities under the Privacy Rule
 - e. Role of the Privacy Officer and reporting employee and patient concerns regarding privacy issues
 - f. Importance of and benefits of privacy compliance
 - g. Consequences of failure to follow established privacy policies
 - h. Use of the Company’s specific privacy forms
 - i. Submission of patient care reports

COMPANY NAME

PRIVACY POLICY TRAINING CHECKLIST

Training conducted on _____ by _____.
Date Name of Instructor

Attendees included those persons on the Training Documentation Form.

Training included: (Please check next to action item to indicate training completion.)

- _____ Introduction to HIPAA and the Privacy Rule
- _____ Introduction for Privacy Officer and Overview of Privacy Officer Responsibilities
- _____ Explanation of Workforce Confidentiality Agreements
- _____ Overview of Company's Privacy Policies and Procedures
- _____ Overview of Company's Notice of Privacy
- _____ Explanation of Privacy Forms
 - _____ Patient Authorization Form
 - _____ Form Requesting Restriction on Uses and Disclosures of PHI
 - _____ Form to Inspect and Copy PHI and to Implement Access Denial
 - _____ Form to Amend PHI
 - _____ Form to Receive Accounting of Disclosures of PHI
 - _____ Patient Complaint Form
- _____ Explanation of Who Can Disclose PHI
- _____ Discussion of Job Responsibilities as it Relates to PHI
Submission of Patient Care Reports

Draft

Access to PHI – Patient Request to Inspect and Copy, Model Policy

This section of the privacy manual addresses a patient's request to inspect, copy, or amend his or her protected health information maintained by "Company Name."

Patient Requests for Access to Protected Health Information

A patient or a patient's representative may inspect and obtain a copy of his or her information maintained in medical records or other information systems of Company Name.

Procedures – Patient Request for Protected Health Information

- A patient must submit a request to inspect or copy protected health information.
- The request will be reviewed.
- If the request is denied, the patient will be informed.
- If the request is approved, the patient will be given access to the requested information.

Submission of Request for Access to Protected Health Information

A patient must request an opportunity to inspect or copy his or her protected health information.

Procedures – Request for Access to Protected Health Information

- When a patient or patient's representative orally requests access to information, he or she should be told that all requests to inspect or copy protected health information must be submitted in writing. The patient should be referred to Office Manager.
- The designated officer will give the patient or patient's representative a copy of the request form and explain the Company's policies on allowing a patient to inspect his or her records.
- Upon receipt of a request form, the Privacy Officer will review the request,

Review of Patient Requests for Access to Protected Health Information

The request for access to personal health information will be sent promptly to Privacy Officer. A copy of the request will be filed in the patient's records.

The Privacy Officer will consider the restrictions on access listed below when determining whether to approve or deny the request to inspect or copy protected health information.

Draft

A decision to grant the patient or patient's personal representative permission to inspect or copy the requested information will be made within seven (7) days of the date on which the request is submitted, as required by federal and state laws. The more stringent requirement prevails when there is a difference between the two.

Restrictions on Access

Information compiled in anticipation of, or for use in, legal proceedings will not be made available to the patient or patient's legal representative unless required by law or court order.

- Information that, by law, may not be disclosed to the patient will not be made available to the patient or patient's representative.
- Information will not be made available if the patient's physician believes that it is likely to endanger the life or physical safety of the patient. This denial may be appealed.
- Information will not be made available if the company believes that access to the information is reasonably likely to cause substantial harm to a person other than the patient who is referenced in the patient's records. This denial may be appealed.
- Information will not be made available to a personal representative of the patient if the patient's physician believes that access to the information by the personal representative is reasonably likely to cause harm to the patient or to another person. This denial may be appealed.

Procedures – Restriction of Access to Protected Health Information

- The Privacy Officer will review the request to inspect or copy protected health information.
- If the request is disapproved, wholly or in part, the patient will be notified according to Company's policy
- If the request is approved the patient will be notified and arrangements made for the patient to inspect or copy the requested information

Denial of Requests

If a patient's request to inspect or copy protected health information is denied, wholly or in part, the patient will be contacted and given an opportunity to request a review of that decision. The review may be denied if it is prohibited by law.

Draft

A written explanation of the denial of a patient's request to inspect or copy protected health information will be provided to the patient. The following elements must be included in the denial:

- written in plain language.
- reason for denial.
- statement of the individual's review rights.
- description of the complaint process.
- describe alternatives if available.

If alternative information can be identified that may partially satisfy the patient's request, including a summary of the requested information, the communication should describe those alternatives.

Review of Decision to Deny Access

A patient or patient's representative whose request to inspect or copy protected health information is denied may request a review of that decision by a licensed health professional who was not involved in the decision to deny the request.

Procedures – Review of Denial to Provide Access to Protected Health Information

- When the Privacy Officer receives a patient request for a review of the denial, he or she should forward the request to another provider within the Company who was not involved in the original denial, and should ask that provider to review the decision.
- The review should normally be completed within 30 days. The Privacy Officer will follow-up with the reviewing provider if the review is not completed within 30 days of sending him or her the request.
- The Privacy Officer should communicate the result of the review to the patient using the reviewer form.

Inspection of Records

If the records must be retrieved from off-site storage, the patient should be notified that the requested information will be made available, generally within 60 days of the date the request was made.

Draft

Communication of Decision Regarding Inspection/Copying of Protected Health Information

Approval of a patient's request to inspect or copy protected health information should be communicated to the patient or patient's representative using the request approval form.

The form should specify the earliest date and time that the records will be available for copying.

Procedure – Communication of Decision

- The Privacy Officer will determine the earliest date at which the requested information can be made available.
- The Privacy Officer or a designated staff person will prepare the approval form and send it to the patient.

Arrangements for Inspection

Arrangements should be made to provide access to protected health information at a place and time convenient for the patient.

The patient must inspect the records on the premises of the Company. If this is not satisfactory to the patient, he or she should be given the option of having copies made and sent to an address that he or she specifies. However, the patient must pay for such copies as outlined in this policies and procedures manual.

Fees for Copying Personal Health Information

If the patient requests copies of personal health information maintained by the Company, he or she may be charged a fee.

Draft

Access to PHI – Patient Request to Inspect and Copy, Model Forms

COMPANY NAME

REQUEST TO INSPECT AND COPY PROTECTED HEALTH INFORMATION

Patient Name: _____

Date of Birth: _____

Patient Address: _____
Address 1

Address 2

City, State Zip

I understand and agree that I am financially responsible for the following fees associated with my request: copying charges, including the cost of supplies and labor, and postage related to the production of my information. I understand that the charge for this service is \$_____ per page, with a minimum charge of \$_____.

Signature of Patient or Legal Guardian

Date

Print Name of Patient or Legal Guardian

COMPANY NAME

PATIENT DENIAL LETTER

Date

Patient's Name

Address

City, State, Zip

Dear _____:

In accordance with the Final Rule for the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) issued by the U.S. Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), _____ (company name) is unable to honor your request to inspect and obtain a copy of your protected health information (PHI) for the following reason(s):

- _____ does not possess the information requested. **[Insert location of PHI, if known]**

- The Privacy Rule does not require the Company to permit you to inspect and obtain a copy of the requested information because it has been compiled in anticipation of, or for use in a civil, criminal or administrative action or proceeding.

- The Privacy Rule does not require the Company to permit you to inspect and obtain a copy of the requested information because the information was obtained from someone other than a healthcare provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

- A licensed healthcare professional has determined in his/her professional judgment that access to the requested information is reasonably likely to endanger your life or physical safety or the life or physical safety of another person.
- The requested information makes reference to another person and a licensed healthcare professional has determined, in the exercise of reasonable judgment, that the requested access is reasonably likely to cause substantial harm to such other person.
- You are the personal representative of the subject of the requested information, and a licensed healthcare professional has determined, in the exercise of professional judgment, that the requested information should not be provided to you.

If access to requested information has been denied for any of the last three reasons listed above, you have the right to have the denial reviewed by another licensed healthcare professional who did not participate in this denial. If you choose to have this denial reviewed, please submit a written request to our contact person at:

Name of Privacy Officer _____

Company Name _____

Address _____

City _____ State _____ Zip _____

Our Privacy Officer will respond with a written decision within a reasonable period of time whether or not to ultimately grant or deny access to your PHI as originally requested. You may file a complaint regarding this denial with the Privacy Officer at (telephone #) or with the Secretary of the US. Department of Health and Human Services. Complaints to the Secretary must be in writing, name the Company, describe the acts/omissions believed to violate the Privacy Rule, and be filed within 180 days of the alleged violation.

Very truly yours,

Name and Title

Draft

Patient Request to Amend or Correct PHI, **Model Form**

COMPANY NAME

REQUEST FOR CORRECTION/AMENDMENT OF PROTECTED HEALTH INFORMATION

Patient Name _____

Date of Birth: _____

Patient Address: _____

Address 1

Address 2

City, State Zip

Type of Entry to be Amended:

Please explain how the entry is inaccurate or incomplete.

Please specify what the entry should say to be more accurate or complete.

Signature of Patient or Legal Guardian

Date

FOR INTERNAL PURPOSES ONLY:

Date Request

Amendment has been: Accepted

Denied

Denied in part, Accepted in part

If denied (in whole or in part)*, check reason for denial:

Draft

- PHI was not created by this organization.
- PHI is not available to the patient for inspection in accordance with the law.
- PHI is not a part of patient's designated record set.
- PHI is accurate and complete.

Comments from healthcare provider who provided service:

Name of Staff Member Completing Form: _____

Title: _____

Signature of Healthcare Provider Who Provided Service

Date

*If your request has been denied, in whole or in part, you have the right to submit a written statement disagreeing with the denial to the Company, *Attn: {Name of Privacy Officer {Company address}}*. If you do not provide us with a statement of disagreement, you may request that we provide to you copies of your original request for amendment, our denial, and any disclosures of the protected health information that is the subject of the requested amendment. Additionally, you may file a complaint with our Privacy Officer *[insert name or title, and telephone number]* or the Secretary of the U.S. Department of Health & Human Services.

*COMPANY MUST INFORM PATIENT THAT A WRITTEN REQUEST IS REQUIRED, AND THAT THE PATIENT IS REQUIRED TO PROVIDE A REASON TO SUPPORT THE REQUESTED CHANGE.

Patient Request for an Accounting of Certain PHI Disclosures, Model Form

COMPANY NAME

**REQUEST FOR AN ACCOUNTING OF CERTAIN DISCLOSURES OF
PROTECTED HEALTH INFORMATION FOR NON-TPO PURPOSES**

As a patient, you have the right to receive an accounting of certain non-routine disclosures of your identifiable health information made by our Company for non-TPO purposes. Your request must state a time period that may not be longer than six (6) years and may not include dates before April 14, 2003. The first list you request within a 12-month period will be provided free of charge. For additional lists during the same 12-month period, you may be charged for the costs of providing the list; however the Company will notify you of the cost involved and you may choose to withdraw or modify your request. You are allowed to request a specific disclosure or you may request all disclosures that are required to be included in the accounting.

To request an accounting of disclosures for non-TPO purposes made by the Company, you must submit your request in writing to *{Name, Address, Phone Number of Privacy Officer}*.

Patient Name: _____

Date of Birth: _____

Patient Address: _____

Address 1

Address 2

City, State Zip

Signature of Patient or Legal Guardian

Date

Draft

Patient Request for an Accounting of Certain PHI Disclosures, Model Log

<div style="background-color: yellow; width: 50%; margin: 0 auto; height: 20px; border-bottom: 3px double black;"></div> <p>COMPANY NAME</p> <p>LOG TO TRACK DISCLOSURES OF PHI (PATIENT SPECIFIC)</p> <p>PATIENT NAME _____</p>

For each patient, you are required to keep a log of all disclosures of PHI for non-TPO reasons for which you did not receive a signed authorization from the patient. For each disclosure, fill in the date it occurred along with a description of the type of disclosure. In addition, you need to provide a description of the PHI disclosed along with the names and titles to whom it was disclosed.

DATE	DESCRIPTION OF DISCLOSURE	DESCRIPTION OF PHI	Who Requested	To Whom PHI Was Disclosed	Approve/Deny (+ initials)	REASON FOR DENIAL, COMMENTS

Note: The company must retain related documentation and tracking log for each patient for six (6) years from the date of its creation or the date when it last was in effect, whichever is later.

Draft

Patient Complaints, Policy

The Administrative Requirements section of the HIPAA Privacy Rule requires that a covered entity designate a contact person or office to be responsible for receiving complaints regarding its privacy . Covered entities must document any complaints and their disposition, if any, and retain these records for six years. Covered entities may not threaten, intimidate or retaliate against any individual who files a complaint.

Facilitating Investigations Arising From a Complaint

If, as a result of a complaint to the Secretary of HHS, a covered entity is investigated, the covered entity must permit access to information during normal business hours (or at any time and without notice, if the Secretary determines that the circumstances warrant). Additionally, business associates of such covered entity are also required, pursuant to business associate agreements, to make information available to the Secretary for such investigations.

You have a right to file a complaint if you believe your privacy rights have been violated. You may file a complaint with our **Company** or with the Secretary of the Department of Health and Human Services. To file a complaint with our Company, contact **[insert the name, title, and phone number of the contact person or office responsible for handling complaints]**. All complaints must be submitted in writing. You will not be penalized for filing a complaint.

Draft

Patient Complaints, **Model Company Form**

PATIENT COMPLAINT FORM

Our Company values the privacy of its patients and is committed to operating our Company in a manner that promotes patient confidentiality while providing high quality patient care.

If the staff at **(Company)** have fallen short of this goal, we want you to
Company Name

notify us. Please be assured that your complaint will be kept confidential. Please use the space provided below to describe your complaint. It is our intent to use this feedback to better protect your rights to patient confidentiality.

Name of Patient

Date

Signature of Patient

Phone Number

All complaints must be retained on file for six years.

Draft

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is distributed with the understanding that the Eastern PA EMS Council is ***not*** engaged in rendering any legal or professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

For more information see:

Federal Register, Part II, Department of Health and Human Services, Office of the Secretary, 45CFR parts 160 and 164, Standards for Privacy of Individually Identifiable Health Information; Final Rule

<http://www.hipaalive.com>

www.hhs.gov/ocr/hipaa/

www.nhvship.org

http://www.wedi.org/public/articles/HIPAA_GLOSSARY.pdf

new all required policies