

# PRIVACY POLICY



Last Revision Date  
5/26/20  
Version 4

Document Owner  
Orlando Gonzalez, ADHI

## **Introduction**

- Purpose
- Scope
- Definitions

## **Section 1- Privacy Policies and Procedures**

- 1.1 Designation of Privacy Official
- 1.2 General Associate Responsibilities
- 1.3 Training and Education
- 1.4 Reporting of Suspected Violations of Privacy Policies and Procedures
- 1.5 Investigation of Potential Privacy Violations by Associates
- 1.6 Sanctions and Penalties
- 1.7 Business Associates
- 1.8 Development and Maintenance of Privacy Policies and Procedures
- 1.9 Identifying Protected Health Information
- 1.10 Safeguards
- 1.11 Minimum Necessary
- 1.12 Designation of Record Sets
- 1.13 Documentation and Record Keeping
- 1.14 Routine and Recurring Disclosures of Protected Health Information
- 1.15 Use and Disclosure of Mental Health Information
- 1.16 Consent for Uses and Disclosures Permitted
- 1.17 Use and Disclosure of Protected Health Information for Treatment Purposes
- 1.18 Use and Disclosure of Protected Health Information for Payment Purposes
- 1.19 Use and Disclosure of Protected Health Information for Health Care Operations
- 1.20 Use and Disclosure of Protected Health Information for Health Oversight Activities
- 1.21 Disclosures of Protected Health Information Relating to Judicial and Administrative Proceedings
- 1.22 Use and Disclosure for Specialized Government and Law Enforcement Officials
- 1.23 Disclosures of Protected Health Information Relating to Communicable Diseases
- 1.24 Use or Disclosure for Sale of Protected Health Information
- 1.25 Use and Disclosure for Marketing and Fundraising
- 1.26 Use and Disclosure for Facility Directories
- 1.27 Other Uses and Disclosures of Protected Health Information
- 1.28 Communications and Media Relations
- 1.29 Offshoring Information Outside the United States
- 1.30 Publishing Confidential Information
- 1.31 Notice of Privacy Practices
- 1.32 Verification of the Identity and Authority of a Consumer Requesting Disclosure of Protected Health Information
- 1.33 Authorization of Use or Disclosure
- 1.34 Consumer Requests for Restrictions on Uses and Disclosures of Confidential Communications
- 1.35 Facsimile Transmission of Protected Health Information
- 1.36 Personal Representatives
- 1.37 Parental Access to Protected Health Information Concerning Children
- 1.38 Disclosure of Information to Family Members
- 1.39 Consumer Access to Protected Health Information
- 1.40 Amendment of Health Information
- 1.41 Accounting to Consumers for Disclosure of Information
- 1.42 Submission of Complaints
- 1.43 Complaint Resolution Procedures
- 1.44 Mitigation
- 1.45 Non-retaliation and Protection for Whistleblowers

## **Section 2- Breach Incident Management Policies and Procedures**

- 2.1 Mobile Device Inventory

- 2.2 Mobile Device Protection
- 2.3 Confidential Information
- 2.4 Risk Analysis
- 2.5 Discovery of a Breach
- 2.6 Risk Assessment
- 2.7 Breach Incident Investigation
- 2.8 Breach Reporting by Business Associate
- 2.9 Breach Notification to Individuals
- 2.10 Breach Notification to Office for Civil Rights (OCR)
- 2.11 Breach Notification to States
- 2.12 Breach Notification to Law Enforcement Delay

**Section 3- Conducting Internal HIPAA Audits**

- 3.1 Deciding What Information to Audit
- 3.2 Audit Plan
- 3.3 Conducting the Audit
- 3.4 Reporting Audit Findings
- 3.5 Privacy and Security Auditing

**Section 4- Unique Identifier Policies and Procedures**

- 4.1 Consumer Identifiers
- 4.2 Provider Identifiers

**Appendix A- Privacy Forms**

- EHN Privacy Policy Organizational Chart
- List of Privacy Related Positions
- Sample Business Associate Agreement
- Notice of Privacy Practices
- Consent to Release Information
- Confidential Communication Request Form
- 42 CFR Part 2- Requisite Language
- Texas Family Code Section 32.004
- Research Request Application

**Appendix B- Breach Reporting**

- Privacy Breach Assessment
- Sample Breach Notification Letter
- Reporting a Possible Breach

---

# Introduction

## Purpose

This policy defines controls to safeguard the protected health information of Emergence Health Network consumers. Ensure the integrity and compliance of federal and state regulations as it pertains to protected health information. It serves as a central policy document with which all employees and contractors must be familiar; and defines actions and prohibitions that all users must follow. The policy provides Emergence Health Network with policies and guidelines concerning the access, disclosure, use, breach notification, investigations, and audits of protected health information. Ensuring that communication between EHN associates, consumers, and consumer families occurs timely and is the least restrictive to effective treatment. Effective treatment of consumers is achieved by eliminating re-traumatizing practices that are often used in many service systems. EHN has incorporated a trauma-informed culture by making change to its policies and procedures; staff trainings; and interventions. This trauma informed culture gives the client shared decision making, choice, and goal setting of their treatment.

## Scope

This policy applies to all Center Associates responsible for creating, managing, storing and the disclosing of consumer protected health information.

Policy:

It is the policy of Emergence Health Network (EHN) that all operations involving the receipt, handling, maintenance and disclosure of any individually-identifiable information regarding the treatment, care, and billing of EHN consumers are performed in accordance with federal and state patient privacy laws including, but not limited to, the Health Insurance Portability and Accountability Act (HIPAA), Chapters 181 and 611 of the Texas Health and Safety Code, and 42 CFR Part 2 (where applicable). The Chief Executive Officer of EHN shall update existing procedures to ensure compliance with federal and state patient privacy laws.

## Definitions

### **Affiliated Covered Entity**

Legally separate affiliated Covered Entities may be designated as a single Covered Entity for purposes of HIPAA Privacy if the separate entities are under common ownership or control.

### **Business Associate**

A Business Associate includes an entity that “creates, receives, maintains, or transmits” protected health information on behalf of a Covered Entity. Entities that maintain or store protected health information on behalf of a Covered Entity are Business Associates, even if they do not actually view the protected health information.

Examples of Business Associates:

- Patient Safety Organizations

- Health Information Organizations
- Vendors of Personal Health Records that require routine access to PHI
- Persons who facilitate data transmission
- Data storage company that has access to PHI (whether digital or hard copy), even if the entity does not view the information
- Subcontractors that create, receive, maintain, or transmit PHI on behalf of the Business Associate.

Examples of persons and organizations not considered Business Associates:

- Oversight agencies (OIG, CMS)
- A person or organization that acts merely as a conduit (a conduit transports information but does not access it, ex: United States Postal Service)
- Financial institutions
- Health care providers
- Employees of a Covered Entity

**“Certain” Health Care Operations**

“Certain” Health Care Operations means any of the following activities performed or undertaken by another Covered Entity requesting a disclosure from EHN.

- Quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines
- Population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination
- Contacting patients regarding information about treatment alternatives
- Reviewing the competence or qualifications of health care professionals
- Evaluating provider performance
- Evaluating health plan performance
- Accreditation
- Certification
- Licensing
- Credentialing
- Health care fraud and abuse detection or compliance

**Covered Entities**

Health plans, health care clearinghouses, and health care providers.

**Disclosure (Disclose)**

Release, transfer, provide access to, or divulge in any other manner of information outside of EHN.

**Electronic Media**

Includes any electronic storage material as defined by NIST. Thus, “intranets” come within the definition. PHI stored, whether intentionally or not, in a photocopier, facsimile, or other device is subject to the Privacy and Security Rules. Exception: If the information exchanged by facsimile did not exist in electronic form immediately before transmission, that information is not electronic media.

**Employee**

For purposes of the Privacy policies, the definition of employee includes all EHN workforce members including interns and temporary personnel. See also “Workforce Member” below.

**Group Health Plan**

An employee welfare benefit plan defined in section 3(1) of ERISA, 29 U.S.C. 1002(1), including insured and self-insured plans to the extent the plan provides medical coverage to employees or their dependents directly or through insurance, reimbursement, or otherwise, and has 50 or more participants or is administered by an entity other than the employer that established and maintains the plan.

**Health Care Operations**

- Health Care Operations means any of the following activities performed or undertaken by EHN:
  - Conducting quality assessment and improvement activities
  - Accreditation
  - Credentialing
  - Certification
  - Case management
  - Licensing
  - Evaluating health plan performance
  - Patient safety activities as defined in the PSQIA
  - Prohibition on using or disclosing genetic information for underwriting purposes
  - Insurance activities relating to the renewal of a contract for insurance:
    - Underwriting
    - Premium rating
    - Other activities relating to the creation, renewal or replacement of a

contract for health insurance or health benefits, as well as ceding, securing or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss and excess loss insurance)

- Note: A group health plan that wants to replace its insurance carrier may disclose certain PHI to insurance issuers in order to obtain bids on new coverage, and an insurance carrier interested in bidding on new business may use PHI obtained from the potential new client to develop the product and price.
  - Conducting or arranging for medical review
  - Auditing functions, including fraud, abuse detection, and compliance programs
  - Conducting or arranging for legal services
  - Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment, or coverage policies
- Business management activities and general administrative functions, such as:
  - Management activities relating to implementation of and compliance with the requirements for health care operations
  - Customer service, including the provisions of data analyses for policyholders, plan sponsors, or other customers, provided PHI is not disclosed to such policyholder, plan sponsor, or customer
  - Resolution of internal grievances (includes quality of care and internal employee complaints)
  - Due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a Covered Entity or, following completion of the sale or transfer, will become a Covered Entity
- Activities that would not be considered health care operations:
  - Marketing of health and non-health items and services;
  - Disclosure of PHI for sale, rent, or barter;
  - Use of PHI by a non-health related division of an entity; or
  - Disclosure to an employer for employment determinations.

### **Health Information**

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

- Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school, university or health care clearinghouse.

- Relates to the past, present, or future physical or mental health or condition of a patient; the provision of health care to a patient; or past, present or future payment for the provision of health care to a patient.

“Health Information” includes genetic information.

### **Health Plan**

An individual or group plan that provides or pays the cost of medical care, including church plans and government plans. (Any plan to which creditable coverage applies.)

### **Individually Identifiable Health Information**

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

- Is created or received by a Covered Entity.
- Relates to the past, present, or future physical or mental health or condition of a patient; the provision of health care to a patient; or past, present or future payment for the provision of health care to a patient:
  - Which identifies the patient; and
  - With respect to which there is a reasonable basis to believe the information can be used to identify the patient.

### **Organized Health Care Arrangement**

- A clinically integrated care setting in which patients typically receive health care from more than one health care provider.
- An organized system of health care in which more than one Covered Entity participates, and in which the participating Covered Entities hold themselves out to the public as participating in a joint arrangement and participate in joint activities that include at least one of the following:
  - Utilization review, in which health care decisions by participating Covered Entities are reviewed by other participating Covered Entities or by a third party on their behalf.
  - Quality assessment and improvement activities in which treatment provided by participating Covered Entities is assessed by other participating Covered Entities or by a third party on their behalf.
  - Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating Covered Entities through the joint arrangement and if PHI created or received by a Covered Entity is reviewed by other participating Covered Entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.
- A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to PHI created or received by such health insurance issuer or HMO that relates to patients who are or who have been participants or beneficiaries in such group health plan.
- A group health plan and one or more other group health plans, each of which are maintained by the same plan sponsor.

- The group health plans described in number 4 above and health insurance issuers or HMOs with respect to such group health plans, but only with respect to PHI created or received by such health insurance issuers or HMOs that relates to patients who are or have been participants or beneficiaries in any of such group health plans.

### **Payment**

- The activities undertaken to:
  - Obtain premiums or determine or fulfill our responsibilities for coverage and provision of benefits.
  - Obtain or provide reimbursement for the provision of health care.
- The activities that relate to the patient receiving health care include, but are not limited to:
  - Determinations of eligibility or coverage (including coordination of benefits) and adjudication or subrogation of health benefit claims;
  - Adjusting premium amounts due based on enrollee health status and demographic characteristics (this is aggregate data used to rate an entire group);
  - Billing, claims management, collection activities, or obtaining payment under a contract for reinsurance (including stop-loss);
  - Medical necessity review; and
  - Utilization review activities (preauthorization).
- EHN may disclose to consumer reporting agencies any of the following PHI relating to collection of premiums or reimbursement: a patient's name, address, date of birth, Social Security number and payment history, account number, and name and address of the patient's health care provider and/or health plan.

### **Plan Sponsor**

Plan sponsor is defined in section 3(16) (B) of ERISA, 29 U.S.C. 1002(16) (B). The plan sponsor is the employer or employee organization (in the case of an employer benefit plan) established or maintained by an employer (includes church and government plans). The plan sponsor is responsible for setting up the plan and regulatory reports and retains the right to amend the plan and sign official plan documents. The plan sponsor is limited to assigned responsibilities.

### **Protected Health Information (PHI)**

All individually identifiable health information transmitted or maintained by a Covered Entity, regardless of form.

The HIPAA Privacy and Security Rules do not protect the individually identifiable health information of persons who have been deceased for more than 50 years.

### **Psychotherapy Notes**

Notes recorded by a health care provider who is a mental health professional documenting conversation for analysis during a private counseling session or a group, joint, or family counseling session. The information must be separated from the rest of the patient's medical record.

### **Subcontractor**

A person who acts on behalf of a Business Associate, other than in the capacity of a workforce member of the Business Associate. The Covered Entity is not required to have a contract with the subcontractor. The Business Associate is required to obtain satisfactory assurances from the subcontractor in the form of a written contract or other arrangement that a subcontractor will appropriately safeguard PHI.

### **Telecommuting**

Telecommuting, also called telework, teleworking, working from home, mobile work, remote work, and flexible workplace is a work arrangement in which employees do not commute or travel to a central place of work, such as an office building, warehouse, or store. Teleworkers often use mobile telecommunications technology such as a Wi-Fi-equipped laptop or tablet computers and smartphones to work.

### **Treatment**

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

### **Underwriting Purposes**

In this context, “underwriting” refers to a group health plan, health insurance coverage, or Medicare supplemental policy. Examples of “underwriting purposes” are:

- Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy. This includes changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program.
- The computation of premium or contribution amounts under the plan, coverage, or policy.
- Includes discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program.
- The application of any pre-existing condition exclusion under the plan, coverage, or policy.
- Other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits.

“Underwriting Purposes” does not include determinations of medical appropriateness where an individual seeks a benefit under the plan, coverage, or policy.

### **Use**

The employment, application, utilization, examination, or analysis of individually identifiable health information within an entity (EHN) that maintains the information.

### **Workforce Member**

The term includes employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a Covered Entity or a Business Associate, is under the direct control of the Covered Entity or Business Associate.

---

# Section 1—Privacy Procedures

This section includes policies and procedures as part of Emergence Health Network’s consumer (patient) privacy compliance program.

## 1.1 Designation of Privacy Official

Emergence Health Network will designate a privacy official as required under state and federal patient privacy laws and regulations.

### **Procedure**

The Administrative Director of Health Information is responsible for the development and implementation of policies and procedures to safeguard the privacy of consumers’ health information consistent with federal and state laws and regulations.

The specific responsibilities of the Administrative Director of Health Information include:

- Developing policies and procedures as provided in **section 1.8**
- Developing and conducting training programs on privacy policies and procedures
- Responding to questions from associates and consumers concerning privacy policies and procedures
- Receiving complaints concerning the privacy practices described in the notice of privacy practices as described in **section 1.42**
- Auditing compliance with privacy policies and procedures
- Investigating and correcting violations of privacy policies and procedures

The Administrative Director of Health Information may assign any of these responsibilities to other Associates or contractors but is responsible for making sure these responsibilities are carried out.

## 1.2 General Associate Responsibilities

Emergence Health Network will create assurances that all associates act in an appropriate and compliant manner to protect consumer information under the HIPAA privacy regulations.

### **Procedure**

All Associates are responsible for safeguarding the privacy of consumer health information.

An organizational chart of positions relevant to the compliance of this privacy policy is in Appendix A. A list of privacy related positions with names is located in Appendix A.

All Associates must:

- Use and disclose protected health information only as authorized in their job description or as authorized by a supervisor
- Conduct oral discussions of personal health information with other associates or with consumers and family members in a manner that limits the possibility of inadvertent disclosures
- Complete a privacy training (see **section 1.3**)
- Report suspected violations of a business associate's contractual obligations to safeguard protected health information (see **section 1.7**)
- Report suspected violations of the policies and procedures established in this manual by Associates as detailed in **section 1.6**

These requirements may be satisfied by referring to standard job classes the Administrative Director of Health Information may establish under **section 1.19, "Use and Disclosure of Protected Health Information for Health Care Operations,"** definitions of the positions authorized to routinely use or disclose standard categories of protected health information.

## 1.3 Training and Education

Emergence Health Network will ensure that all associates are trained regarding the HIPAA privacy regulations and our organization's privacy practices and that any revisions in the policies will be communicated via trainings and or notices.

### **Procedure**

The Administrative Director of Health Information or Associates designated by the Administrative Director of Health Information will develop a privacy policy orientation and training program.

This purpose of this program is to make sure that all EHN employees and contractors (herein, Associates are familiar with the privacy policies and procedures adopted by Emergence Health Network.

The training and orientation program will cover:

- The definition and identification of protected health information
- How to provide the notice of privacy practices to all consumers and obtain a written acknowledgment of receipt
- Use and disclosure of protected health information for treatment, payment, and health care operations
- How to obtain authorization, when required, for use and disclosure of protected information
- Procedures for handling suspected violations of privacy policies and procedures
- Penalties for violations of privacy policies and procedures
- Documentation required by the policies and procedures manual

Associates will:

- Receive a summary of EHN's privacy policies and procedures
- Have an opportunity to review the policies and procedures manual
- Have an opportunity to ask questions about the privacy policies and procedures of Emergence Health Network

All Associates must complete the privacy policy orientation and training program during their probationary period.

- Completion of the privacy policy orientation and training program will be documented in the employee's personnel file by the Administrative Director of Health Information or the Associates who conducts the training.
- Until Associates complete the privacy policy orientation and training program, their supervisors will closely monitor their use and disclosure of protected health information.
- Before the end of an Associates probationary period, his or her supervisor should confirm that he or she has completed privacy training.
- The probationary period of any new employee who has not completed the privacy policy orientation and training program will be extended. In some cases, an employee who does not complete the privacy orientation and training program before the end of his or her probationary period will be required to complete the program before resuming normal job duties.

If privacy policies are revised, or if there is a change in regulations requiring additional training, the Administrative Director of Health Information or an Associate designated by the Administrative Director of Health Information will develop training materials on new or revised privacy policies and procedures.

- Associates whose job responsibilities are affected by a change in privacy policies and procedures must complete training on the revised policies and procedures within one month of their effective date.
- Completion of training on revised policies and procedures will be documented.

## 1.4 Reporting of Suspected Violations of Privacy Policies and Procedures

Emergence Health Network employees and associates will be responsible for reporting any suspected violations of privacy policies or procedures.

### **Procedure**

All Associates should report possible violations of privacy policies and procedures to their supervisor or via EthicsPoint. If the supervisor determines that a violation occurred or that the situation warrants further investigation, the possible violation should be reported to the Administrative Director of Health Information.

Under the following circumstances, an Associate should not report potential violations to his or her supervisor and/or the Administrative Director of Health Information:

- Violations involving the Associates supervisor should be reported directly to the Administrative Director of Health Information.
- Violations involving the Administrative Director of Health Information should be reported to the Chief Information Officer.
- Associates always have the right to contact the Department of Health and Human Services Office for Civil Rights directly as well, at [OCRcomplaint@HHS.gov](mailto:OCRcomplaint@HHS.gov).
- Reportable offenses include use and disclosure of protected health information that may violate:
  - The practices described in the notice of privacy practices form
  - A consumer's authorization

Discussion of protected health information in public areas should be reported only if the discussion involves the disclosure of a substantial amount of protected health information and it would have been practical to conduct the discussion in a private area.

Associates reporting a violation should describe the possible violation in writing or should arrange a meeting with the supervisor and/or Administrative Director of Health Information to discuss the possible violation.

## 1.5 Investigation of Potential Privacy Violations by Associates

All potential privacy violations will be investigated by the Administrative Director of Health Information or a delegate assigned by the Administrative Director of Health Information.

### **Procedure**

Upon being notified of a potential violation of privacy policies and procedures by Associates or consumer (under **section 1.42**), the Administrative Director of Health Information will:

- Review any documentation
- Meet with the Associates or consumer who reported the possible violation
- Meet with the Associates who may have violated the policies and procedures
- Determine what, if any, protected health information was used or disclosed
- Determine whether the use or disclosure violated policies and procedures
- Determine whether the violation was accidental or intentional
- Recommend to the Associates supervisor the disciplinary action, if any, that should be taken
- Document the findings of the investigation and action taken

## 1.6 Sanctions and Penalties

Following a full investigation, appropriate sanctions will be brought against

employees and associates who have been found to have violated the privacy practices of Emergence Health Network.

### **Procedure**

There are two types of violations of privacy policies and procedures:

- Technical violations that do not result in the use or disclosure of protected health information
- Violations that do involve the use or disclosure of protected health information

There also are two types of violations that involve use and disclosure:

- Unintentional or accidental uses or disclosures
- Intentional and deliberate uses and disclosures

Incidental disclosures of information, such as disclosures that occur when a consumer asks a question in a public area, do not need to be reported, documented, or investigated. No sanction will be imposed for incidental disclosures of information. Associates should, nevertheless, make reasonable efforts to minimize incidental disclosures.

The severity of penalties varies with the type of violation. The most severe penalties apply to the intentional disclosure of protected health information in violation of policies and procedures. The least severe penalties apply to unintentional technical violations of policies that do not result in the disclosure of protected health information.

Examples of violations include:

- Technical violations—When obtaining an authorization, Associates fails to notice that the consumer signed but did not date the authorization form.
- Accidental disclosure—Information on the wrong consumer is accidentally sent to a third-party payer.
- Intentional disclosure—Associates provides a drug company representative a list of consumers with an identified medical condition without obtaining the consumer's authorization for this disclosure.

The procedures and penalties that apply to each of these types of violation are defined in **sections 1.6.1–1.6.3** below.

The Administrative Director of Health Information shall establish and maintain files that document all actions taken to impose sanctions under **section 1.6**.

This information shall include:

- A description of, and documenting evidence for, the violation
- A statement clarifying the nature of the violation, specifically indicating whether it was technical or involved the use or disclosure of protected health information, and whether the violation of policies was accidental or intentional
- A description of the sanction that was imposed

An unproven or unsubstantiated allegation of a violation of privacy policies and practices does not have to be documented.

### 1.6.1 Sanctions and Penalties for Technical Violations Not Involving Use or Disclosure

Associates who commit a technical violation of privacy policies and procedures that does not result in any use or disclosure of protected health information will:

- Meet with his or her supervisor to review the policies and procedures that were violated
- Demonstrate to the satisfaction of the supervisor that he or she understands the policies and procedures that should be followed in similar circumstances

The violation will be documented in the Associates personnel file with the Human Resources Department. A pattern of repeated technical violations, even if none result in the inappropriate use or disclosure of protected health information, may result in transfer to another position, suspension, or termination of the Associates per EHN employment policies.

### 1.6.2 Sanctions and Penalties for Unintentional Violations Involving Use and Disclosure

Associates who unintentionally uses or discloses protected health information in violation of the privacy policies and procedures will:

- Meet with his or her supervisor to review the use or disclosure of protected health information that violated EHN's policies and procedures or the Associates authority to use or disclose information
- Demonstrate to the satisfaction of the supervisor that he or she understands the uses and disclosures that he or she is authorized to make under the practice's policies and procedures

The violation will be documented in the Associates personnel file with Human the Resources Department. A pattern of repeated unauthorized use or disclosure of protected health information will result in transfer to another position, suspension, or termination of the Associates per EHN employment policies.

### 1.6.3 Sanctions and Penalties for Intentional Violations Involving Use and Disclosure

The intentional violation of privacy policies and procedures may result in immediate suspension in addition civil or criminal penalties may be imposed, pending further investigation and termination per EHN employment policies. Documentation of the investigation of the violation must show clear evidence that the disclosure of information was intentional and deliberate. That is, the Associates must have disclosed the information knowing that the disclosure violated the policies and procedures of the practice.

If the Associates has previously disclosed the same or similar type of information under the same or similar circumstances, it will be presumed that the disclosure was intentional and deliberate.

## 1.7 Business Associates

Emergence Health Network protects the confidentiality and integrity of health information of its consumers. This procedure defines the guidelines that must be followed for business associates who come into contact with protected health

information.

**Definition:** A business associate is any person or organization that performs or helps perform any function or activity that involves the use or disclosure of protected health information.

In short, any person (other than an employee or other member of the practice staff) or organization that receives transmits or uses protected health information from Emergence Health Network is a business associate. A business associate may receive protected health information from EHN, create protected health information for EHN, or transmit data on behalf of EHN.

Protected health information may be disclosed to business associates only if Emergence Health Network receives satisfactory assurances that the business associate will safeguard the privacy of the protected health information that it creates or receives.

### 1.7.1 Business Associate Agreements

*A sample business associate agreement can be found in appendix A in the back of this manual.*

#### **Procedure**

Written contracts or agreements must be negotiated between an EHN and any business associate that will handle protected health information it receives from or creates for the practice. This contract or agreement must include provisions that:

- Agree to sign a business associate and/or the Texas Health and Human Services (HHS) Data Use Agreement (DUA). The DUA is to facilitate creation, receipt, maintenance, use, disclosure, or access to confidential information with contractor; contractor rights and obligations with respect to the confidential information; the purposes for which the contractor may create, receive, maintain, use, disclose or have access to confidential information; the remedies in the event of non-compliance with its obligations under the DUA.
- Identify the uses and disclosures of protected health information permitted under the contract
- Permit the business associate to use or disclose the information only as permitted under the privacy standards
- Restrict use and disclosure of the protected health information the business associate creates or receives to those that are specified in the contract
- Call on the business associate to fully comply with the provisions of the HIPAA privacy and security regulations, not limited by specific references in the contract with Emergence Health Network
- Provide for reporting to Emergence Health Network any use or disclosure of protected health information not provided for under the business associate's contract
- Require the business associate to apply the same restrictions and conditions on use and disclosure of protected health information to the agents and subcontractors to whom it forwards the protected health information
- Make protected health information available to consumers as provided under **section 1.39**

- Amend any protected health information that it receives when asked to do so by Emergence Health Network
- Make available to Emergence Health Network the information it needs to account for uses and disclosures of protected health information as provided under **section 1.41**
- Make internal practices, books, and records related to the use and disclosure of protected health information available to HHS for the purposes of determining compliance with the privacy standards
- Return, if feasible, all protected health information to Emergence Health Network upon termination of the contract and destroy any copies of such information. When the return and/or destruction of protected health information is not feasible, the business associate will extend contractual protections to the use and disclosure of the information for the purposes that make its return or destruction not feasible.
- Notify Emergence Health Network in the event of an unauthorized disclosure of unsecured PHI
- Provide for termination of the contract if the business associate violates these contractual provisions
- Comply with the privacy rule to the extent the business associate is carrying out the organization's obligations under the privacy rule
- Business associates must enter into business associate agreements with their subcontractors that impose the same obligations that apply to the business associates themselves

### 1.7.2 Duty of Associates to Report Contractual Breaches by Business Associates

#### **Procedure**

If Associates become aware of activities or practices by the business associate that violate EHN's contractual obligations, the activities or practices must be reported to the Administrative Director of Health Information.

### 1.7.3 Investigation and Correction of Contractual Breaches

#### **Procedure**

When the Administrative Director of Health Information is notified that a business associate has violated a contractual provision related to the privacy of protected health information, he or she must implement the following procedure to correct the violation.

- The Administrative Director of Health Information will contact the business associate and determine whether a contractual provision has been violated.
- If a contract provision has been violated, the Administrative Director of Health Information will identify steps to be taken by the business associate that will enable it to comply with its contractual obligations.
- The Administrative Director of Health Information will review the corrective action steps with the business associate and determine whether those steps or other measures suggested by the business associate will correct the violation. If an agreement can be reached, the corrective measures will be summarized

in writing and sent to the business associate.

- The Administrative Director of Health Information will monitor the implementation of the corrective action measures by periodically contacting the business associate. The Administrative Director of Health Information may discontinue monitoring the contract after receiving adequate assurances that the corrective measures have been implemented and that the contract provisions will be complied with in the future.
- If it is not possible to develop an acceptable corrective action plan, the Administrative Director of Health Information should implement the procedures established in **section 1.7.4** to terminate the contract.

#### 1.7.4 Reporting of Contractual Breaches by Business Associates

##### **Procedure**

When the Administrative Director of Health Information is not able to correct violations of contractual obligations by a business associate, he or she should implement the following procedure.

- Identify an alternative source for the services provided by the business associate.
- Refer the matter to the CEO, CIO, CCO and other responsible parties regarding termination of the contract with a request that formal action be taken to terminate the contract.
- Have EHN's legal counsel notify the business associate that action will be taken to terminate the contract if the violation of contract provisions is not immediately corrected.
- Monitor the status of the contract and arrange for replacing the business associate when the contract is formally terminated.

If the contract cannot be terminated, the contract violation should be reported by the Chief Compliance Officer to HHS as required by federal regulations.

### 1.8 Development and Maintenance of Privacy Policies and Procedures

Emergence Health Network is responsible for developing and maintaining in written or electronic privacy policies and procedures pursuant to the HIPAA privacy standards, requirements, implementation specifications, and other subparts.

##### **Procedure**

The Administrative Director of Health Information will develop policies and procedures that are reasonably designed to ensure compliance with federal and state standards for the protection of the privacy of health information. The Administrative Director of Health Information may delegate this responsibility to an Associate, but such delegation must be reflected in that Associates job description, and the Administrative Director of Health Information will supervise the development of all privacy policies and procedures.

The Administrative Director of Health Information must:

- Monitor changes in federal and state law and regulations that may require changes in privacy policies and procedures
- Notify the executive team of the issuance of new or revised federal or state requirements and describe the need to modify policies and procedures, including the date by which revised policies and procedures must be implemented
- Take the initiative to develop new or revised policies and procedures as necessary to meet the requirements of new laws and regulations
- Identify any revisions needed in the privacy orientation and training program to reflect revised policies and procedures

Before a revised policy or procedure is submitted for approval, the Administrative Director of Health Information will review the notice of privacy practices form (see **section 1.31**) and determine whether the notice must be revised to reflect the new privacy policies or procedures.

The effective date of a revised policy or procedure must not be earlier than the date on which the revised notice of privacy practices is posted and made available to consumers.

All policies and procedures must be approved by the executive team of the Administrative Director of Health Information before they can be implemented.

Maintain documentation in writing or electronic communications regarding changes to policies and procedures.

Maintain documentation in writing or electronic of actions, activities, or designations required.

The documentation should be sufficient to meet burden of proof for investigations or inquiries from the Office of Civil Rights or state offices as it relates to use or disclosure violations.

New or revised policies and procedures are to be communicated to Associates through the following:

- An all-staff memorandum from the Administrative Director of Health Information will announce the adoption of the new or revised policies and indicate affected associate's functions. This memorandum should describe the new policy, indicate its effective date, and indicate the date on which the new policy will be available for associate review.
- The Administrative Director of Health Information or a designated representative will announce the adoption of the new policies at appropriate associate meetings and provide appropriate training.
- A memorandum from the Administrative Director of Health Information to those Associates whose job responsibilities are directly affected by the new policies should indicate whether training or orientation meetings or programs will be held and whether background information on the new policies is available. A copy of the revised policy should be attached to the memorandum, or associates should be directed to consult the updated policy and procedure manual.

- Copies of the revised policy will be distributed to Associates for updating their copies of the policy manual.

## 1.9 Identifying Protected Health Information

EHN will treat as PHI any information that relates to a consumer's health condition, identifies a consumer, or for which there is reasonable basis to believe the information can be used to identify the consumer, and limit the use and disclosure of such information.

### **Individually identifiable health information**

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

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

### **Protected Health Information (PHI)**

A consumer's personally identifiable health information that is:

- Transmitted by electronic media;
- Maintained in any medium described in the definition of electronic media; or
- Transmitted or maintained in any other form or medium, including paper and fax documents and oral communications.

### **PROCEDURE**

EHN will protect the use and disclosure of a consumer's individually identifiable health information by treating certain identifiers as PHI. The identifiers pertain to the consumer as well as the consumer's family members, employers or household members and include, but are not limited to:

- Names;
- Geographic designations smaller than a state, including street address, city, county, precinct, and zip code (except that the first three digits of the zip code may be used if the area has more than 20,000 residents);
- All elements of dates (except for year) directly related to a consumer, including birth date, admission date, discharge date, date of death, and age (although the year of age may not be used if the consumer is over 89 unless aggregated into a single category of age 90 or older);
- Telephone numbers;
- Fax numbers;

- Email addresses;
- Social Security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers, serial numbers, and license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs) and Internet Protocol (IP) addresses;
- Biometric identifiers, such as fingerprints;
- Full-face photographs and any comparable images; and
- Any other unique identifying number, characteristic, or code.

If individually identifiable health information is “de-identified,” it is no longer treated as PHI. EHN may de-identify information by removing all identifiers described above.

## 1.10 Safeguards

EHN will establish criteria for safeguarding confidential information and to minimize the risk of unauthorized access, use or disclosure. The safeguards to protect the privacy of protected health information include administrative, technical and physical safeguards.

EHN will take reasonable and appropriate steps to safeguard information from any intentional or unintentional use of disclosure that is in violation of the privacy policies. Information to be safeguarded may be in any format including paper, electronic, oral, or visual mediums of confidential information. Limitation of disclosures should also cover incidental disclosures.

### **PROCEDURE**

Associates will follow the steps to safeguard information based on the combination of information format and location of the confidential information. Onsite location refers to any program or office (clinics, observation unit, residential homes, administrative offices, and/or storage/maintenance facilities) that is operated by Emergence Health Network. Offsite location refers to any locations (hospitals, consumer homes, foster homes, public places, airports, training rooms) not operated by Emergence Health Network.

#### 1.10.1 Safeguarding Confidential Information On-site

##### Paper Format

- Each worksite will store files and documents in locked rooms or storage systems.
- In worksites where lockable storage is not available, Associates must take reasonable efforts

to ensure the safeguarding of confidential information.

- Each workplace will ensure that files and documents awaiting disposal or destruction in desk-site containers, storage rooms, or centralized waste/shred bins, are appropriately labeled, are disposed of on a regular basis, and that all reasonable measures are taken to minimize access (shred bins are locked).
- Each worksite will ensure that shredding of files and documents is performed on a timely basis, consistent with record retention requirements.

#### Mail Format

- Each worksite will ensure that mail is prepared accurately for delivery.
- Outgoing mail must include a complete sending address, including first and last name of recipient, agency name, and complete street and city address. If printed labels are not used, write or print legibly.
- The outgoing mail must also include a complete return address.

#### Oral Format

- Associates must take reasonable steps to protect the privacy of all verbal exchanges or discussions of confidential information, regardless of where the discussion occurs.
- Each worksite shall make enclosed offices and/or interview rooms available for the verbal exchange of confidential information.

Exception: In work environments structured with few offices or closed rooms, such as programs at 1600 Montana Avenue (Outpatient Competency Restoration, Assertive Community Treatment), 1601 Yandell Drive (Central Outpatient Clinic, Extended Observation Unit), or open office environments, uses or disclosures that are incidental to an otherwise permitted use or disclosure could occur. Such incidental uses or disclosures are not considered a violation provided that EHN has met the reasonable safeguards and minimum necessary requirements.

- Each worksite must foster employee awareness of the potential for inadvertent verbal disclosure of confidential information.

#### Visual Format

- Associates must ensure that observable confidential information is adequately shielded from unauthorized disclosure on computer screens and paper documents.
  - Computer screens: Each worksite must make every effort to ensure that confidential information on computer screens is not visible to unauthorized persons. Use of privacy screens on monitors that are in locations where the screen may be visible to consumers or unauthorized is required.
  - Paper documents: Associates must be aware of the risks regarding how paper documents are used and handled and must take all necessary precautions to safeguard confidential information. Taking paper documents (assessments, schedulers/agendas, caseload reports) home is not permitted documents must be left at the worksite in a secure location.

#### Computer/Electronic Format

- Associates who are assigned to use computers or mobile devices are responsible for maintaining the security of passwords or other access methods. Some associates must turn in mobile equipment at the end of the day.

### 1.10.2 Safeguarding Confidential Information Off-site

All the safeguard requirements for the worksite apply equally to any use of confidential information away from or off-site from the workplace. Files and records should be securely transported.

#### Computer/Electronic Format

- Associates authorized to use any EHN owned computing device (e.g., laptop, desktop, tablet, smartphone, etc.) off-site are responsible for assuring the security, as well as minimize the risk of loss of the device and its contents.
- On a case by case basis or under unusual circumstances associates may be given authorization to conduct official EHN business using personal computers for a limited amount of time. Associates should observe security protocols to prevent unauthorized users from accessing confidential information. Lock computer screen when stepping away from the computer when at home or a client's home. Shared use of computers with family member or others who are not part of the work force create a risk of inadvertent disclosure of confidential information.
- Transferring data to personal devices such as computers, tablets, or cell phones is prohibited. Protected health information should not be sent to personal emails or stored in the cloud or thumb drives. Protected health information should not be sent to or from family members devices or accounts.
- Associates are responsible for securing digital camera images. Digital cameras can store confidential information that can be accessed by anyone who has the camera.
- Protected health information should not be posted on any social media platforms.

#### Telephone

- Associates should ensure care when using company issued telephones outside of the worksite. Cell phones, smart phones or other telephones require care to protect confidential information.
- Associates should avoid using identifiable information about clients unless associates have taken reasonable efforts to assure the privacy of the call.
- Transmitting identifiable information about clients is not permitted from or to personal telephones. This can include up to text messaging, descriptions, photographs, or videos.

#### Paper Format

- Associates should not print protected health information in their home. If a circumstance should arise requiring an associate to print at home the associate will need approval from their supervisor and the Privacy Officer.
- Disposal of documents containing protected health information should be done in EHN shredding bins. Documents should not be discarded in trash containers at home, a client's home or public businesses. All protected health information should be protected and stored in a secure area. Documents should also be protected from inadvertent destruction or alteration.

### 1.10.3 Safeguarding Confidential Information through Administrative Methods

Implementation of role-based access and the Minimum Necessary Procedure (see **section 1.11**) will promote administrative safeguards.

- Role Base Access Control (RBAC) is a form of security allowing access to data based on job function in accordance with EHN security procedures. Employees will be assigned to RBAC groups that will give members access only to the minimum necessary information to fulfill their job functions.

Conducting internal reviews periodically will permit EHN to evaluate the effectiveness of safeguards.

- The Health Information Department will conduct reviews, under the directions of the Administrative Director of Health Information, in order to evaluate and improve the effectiveness of their current safeguards.

Compliance with department-wide security policies will enhance administrative safeguards (see Information Security Policy).

Compliance with department-wide privacy policies and program-specific confidentiality and privacy requirements will enhance administrative safeguards.

Training and periodic reminders to EHN Associates about security and privacy are provided in an effort to enhance administrative safeguards.

The established process for responding to security and privacy breaches and investigating causes of breaches permits EHN to continually respond to areas needing improvement and to improve its administrative safeguards, consistent with the Information Security Policy.

### 1.10.4 Safeguarding Confidential Information During Telecommuting

Although telecommuting can be an advantage for users and for the organization in general, it presents risks in the areas of confidentiality and the security of protected health information. Employees connected to EHN's network via a virtual private network become an extension of the wide area network and present additional environments that must be protected against the danger of cybersecurity threats. This arrangement also exposes the corporate as well as protected health information to risks not present in the traditional work environment. In addition to section 1.10.2 the following guidelines need to be followed during telecommuting.

- Take necessary precautions to properly care for any equipment issued for use while engaging in telecommuting. Notify a supervisor immediately of any damaged or lost equipment. Return any equipment issued upon separation from employment.
- Lock computer screen when stepping away from the computer when at home or a client's home. All computers will automatically lock after 3 minutes of inactivity. You can also manually lock a screen by simultaneously pressing *Windows Key+L*. Do not allow family members to use work equipment or access protected health information.
- Transferring data to personal devices such as computers, tablets, or cell phones is prohibited. Protected health information should not be sent to personal emails or stored in the cloud or

thumb drives. Protected health information should not be sent to or from family members devices or accounts.

- Data entry in public locations is not recommended as computer screens can be viewed by individuals in the area of the computer screen.
- Protected health information should be encrypted when sending to an individual that is not an associate of EHN (see **Information Security Policy, Section 4.10 Use of Encrypted Email**). Encryption can be waived only if a consumer requests that the protected health information not be encrypted. EHN associates cannot initiate the conversation about transmitting protected health information without encryption. If an EHN associate receives permission from a consumer to transmit protected health information without encryption the EHN Associate must advise the client of the risks associated with the transmission of unencrypted information. The associate should also document in the client record that they received permission from the consumer.
- Disposal of documents containing protected health information should be done in EHN shredding bins. Documents should not be discarded in trash containers at home, a client's home or public businesses such as gas stations. All protected health information should be protected and stored in a secure area. Documents should also be protected from inadvertent destruction or alteration.

## 1.11 Minimum Necessary

Employees may not use, request, or disclose to others, any PHI that is more than the minimum necessary to accomplish the purpose of the use, request, or disclosure. This includes business information.

EHN shall limit disclosures to the extent practicable to the limited data set, as defined in 45 CFR section 164.514(e)(2), or if needed by the receiving entity, to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

Employees who use PHI not related to their jobs (orally, or from written records or computer terminals) or employees who disclose PHI to any party in violation of this policy or any other privacy policy, shall be subject to disciplinary procedures as per the EHN Sanction Policy including, but not limited to, dismissal. All employees are required to sign and abide by the Employee Confidentiality and Security Agreement.

EHN may rely on a request from another entity for PHI as representing the minimum necessary for the stated purpose, if such reliance is reasonable under the circumstances, and if:

- The request is from a public official.
- The disclosure to the public official must otherwise be permitted under EHN's policies.
- The public official must represent the information requested is the minimum necessary for the stated purpose(s).
- The information is requested by another Covered Entity.
- The information is requested by a professional who is an employee or a Business Associate.
- The purpose of the request is to provide professional services to the Covered Entity.

- The professional represents the information requested is the minimum necessary for the stated purpose(s).

### **Exceptions**

EHN is not limited in the amount of PHI it may disclose to a provider of health care for the purpose of medical treatment.

When federal or state law requires a disclosure of PHI, the minimum necessary information is that which is required to comply with such law. Requests for PHI made by the federal government in the course of a complaint investigation or compliance review and undertaken under Federal Privacy Rule are deemed to meet the minimum necessary rule.

The minimum necessary rule does not apply when disclosing a consumer's PHI to the consumer or the consumer's personal representative.

All information requested within an authorization may be disclosed in accordance with that authorization. This policy does not limit such disclosures.

## **1.12 Designation of Record Sets**

The Access of PHI Policy and Amending PHI Policy permits patients to request access to their Protected Health Information (PHI), receive copies of it, and request certain information be amended. This applies only to information stored in a Designated Record Set.

### **1.12.1 Designated Record Sets are sets of records containing PHI and used to make decisions about individual patients.**

#### **Procedure**

The following are EHN's designated record sets:

- A group of records maintained by or for a Covered Entity that is:
  - The medical and billing records about individuals maintained by or for a covered health care provider;
  - The enrolment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
  - Used, in whole or in part, by or for the Covered Entity to make decisions about individuals.
- For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a Covered Entity."
- The record consists of paper files housed at several locations operated by Emergence Health Network, paper records stored off site and electronic files stored in the electronic health records.

## **1.13 Documentation and Record Keeping**

Emergence Health Network will establish and maintain appropriate systems for

maintenance of documentation under the HIPAA privacy regulations. This documentation will be retained for the appropriate timeframes based on the regulations and Emergence Health Network procedures.

### Procedure

The Administrative Director of Health Information will establish and oversee record-keeping systems to maintain the documentation required by the HIPAA privacy regulations, 42 CFR Part 2 and any other applicable federal or state regulation or law as discussed in various policies throughout this manual.

The information to be maintained in written documentation includes, but is not limited to:

- The policies and procedures contained in this procedure manual
- The notice of privacy practices
- The signed acknowledgment of receipt of the notice of privacy practices
- Signed authorization forms
- Records of recommended disciplinary actions and actions taken against Associates for violations of privacy policies and procedures
- Records of actions taken to enforce compliance with contract provisions by business associates
- Complaint forms received from consumers or other individuals and associated written correspondence
- All requests for an accounting of disclosure of protected health information and records related to such requests
- All requests for amendment of protected health information and records related to the disposition of such requests

#### 1.13.1 Retention of Records

### Procedure

All documentation of actions called for by other policies and procedures contained in this manual will be retained for a minimum of the program regulation from the date the information was created as follows:

Programs Retention Guidelines	
Entity	Minimum Retention Period
Department of Assistive and Rehabilitative Services (DARS)/Early Childhood Intervention (ECI) Program	Five years after the child has been dismissed from services. (40 TAC 108)
Department of Aging and Disability Services (DADS)	Original medical records for a minor until a minor's twenty-fourth birthday or five years from the date of service, whichever is later. (40 TAC 15)
Texas Health and Human Services (HHS)/Department of State Health Services (DSHS)	Seven years past the last date on which services was given or until the consumer's 21 <sup>st</sup> birthday, whichever occurs later. (22 TAC 165)

Adults & Children	
<b>Managed Care Organizations-</b> Superior, Superior Chip, El Paso Health, El Paso Health Chip, Amerigroup, Molina, Amerigroup Medicaid & Medicare Program, Molina Medicaid & Medicare Program, Amerigroup Star Kids, Superior Star Kids	Ten years after the Managed Care Organization contract expires; and/or records are kept longer if they are part of ongoing litigation, audits, claims, or investigations.

In the case of policies and procedures, the retention period will be measured from the date of the most recent revision of the procedure. In other words, when new policies are issued, a copy of the policies that are superseded should be retained for reference purposes for six years following the last day the policy was in effect.

Record Destruction - All hardcopy medical records that require destruction are shredded using National Institute of Standards and Technology (NIST) 800-88 guidelines.

## 1.14 Routine and Recurring Disclosures of Protected Health Information

EHN limits routine and recurring disclosures of PHI to the minimum necessary amount of information that is reasonably necessary to accomplish the purpose of the request or disclosure, in compliance with applicable federal and state laws and regulations.

Some examples of routine and recurring disclosures are:

- To health care providers for claims payment and billing purposes;
- To entities under an Organized Health Care Arrangement for the purposes of Treatment, Payment, Health Care Operations and certain quality improvement activities;
- To a Business Associate under contract to provide specified services; and
- To a plan sponsor and specified consumers for Payment and Health Care Operations of a self-funded plan under an ASO Agreement that permits such disclosure.

Routine and recurring types of PHI disclosure may only occur per the Uses and Disclosures of PHI Policy. Information disclosed in aggregate form that cannot identify an individual consumer is not considered PHI and is not subject to the HIPAA Privacy policies and procedures.

### Reports containing PHI

The Privacy Officer must review all new and revised non-routine and recurring reports that contain PHI being disclosed to an external party prior to the disclosure.

## 1.15 Use and Disclosure of Mental Health Information

### Procedure

EHN and its Associates may use and disclose Protected Health Information related to mental health care. Describe the appropriate use and disclosure of mental health information.

### 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 and that are separated from the rest of the consumer’s medical record. These are records that are kept as private records of a mental health professional. Psychotherapy notes do not include medical records concerning psychiatric or psychological consultations at EHN, or records made by EHN Associates concerning the mental health, well-being, or complaints by

consumers. Psychotherapy notes do not include medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies or treatment furnished, results of clinical tests, and any summary of diagnosis, functional status, the treatment plan, symptoms, prognosis and progress to date.”

#### **Use and Disclosure of Psychotherapy Notes**

EHN Associates will obtain consumer authorization to use or disclose psychotherapy notes, except in the following circumstances:

- The originator of the psychotherapy notes may use those notes for treatment of the consumer.
- EHN Associates, under supervision, may use psychotherapy notes to carry out training programs in mental health. The psychotherapy notes will not be included in the consumer's medical records. The students or trainees in the training programs may examine psychotherapy notes under supervision but will not obtain copies of the psychotherapy notes.
- EHN Associates may use or disclose psychotherapy notes to defend a legal action or other proceeding brought by the consumer.
- EHN Associates will use or disclose psychotherapy notes when they are required by another law to do so.
- EHN Associates will disclose psychotherapy notes to the Secretary of DHHS during DHHS investigations of EHN's compliance with the HIPAA Privacy Standards if DHHS specifically requests to see psychotherapy or mental health professional's personal notes.
- EHN Associates will disclose psychotherapy notes to health oversight agencies if a health oversight agency specifically requests to see psychotherapy notes or the mental health professional's personal notes.
- EHN Associates may disclose psychotherapy notes to coroners and medical examiners regarding deceased consumers if they represent to EHN Associates that those notes are necessary for them to perform their functions.
- EHN Associates may use or disclose psychotherapy notes where necessary to avert a serious and imminent threat to safety. In this circumstance, EHN Associates will first consult with the Compliance Office.

#### **Use and Disclosure of Information Obtained During Court-ordered or Voluntary Evaluation, Examination and Treatment of a Person with a Serious Mental Illness**

All records and other information obtained in the course of evaluation, examination, or treatment of a person subject to the mental health evaluation and treatment provisions are confidential. EHN Associates will disclose these records only as listed in the paragraphs below. If this information includes “psychotherapy notes,” EHN Associates will follow the provisions of paragraph 2 below with regard to the psychotherapy notes only but will follow the provisions of this paragraph regarding all other information.

- EHN Associates may disclose this information to mental health professionals and other providers of health, mental health, or social and welfare services involved in caring for, treating, or rehabilitating the consumer.
- EHN Associates may disclose this information to persons to whom the consumer has given written authorization to receive the information. EHN Associates will use the EHN Release of Information form, or a form that meets the authorization requirements set forth in EHN's policy on authorization.

- EHN Associates may disclose this information to the consumer's legal representative, such as a court-appointed guardian, or the consumer's agent appointed under the consumer's health care directive.
- EHN Associates will have a signed authorization to disclose this information to the consumer's attorney.
- EHN Associates will disclose this information to a person when ordered by a court to do so.
- EHN Associates may disclose this information to a jail/correctional institution if the consumer is an inmate with a county, state or federal jail/correctional institution and an appropriate official represents in writing to EHN Associates the information is necessary for:
  - a) The provision of health care to the consumer;
  - b) The health and safety of the consumer or other inmates;
  - c) The health and safety of officers or employees;
  - d) The health and safety of people transporting inmates;
  - e) Law enforcement on the premises; or
  - f) The administration and maintenance of the "safety, security, and good order of the correctional institution."

If the corrections official cannot make this representation in writing because of the immediate need for such information, EHN Associates will seek such representation verbally and document the representation in the consumer's medical record.

- EHN Associates may disclose limited information to governmental or law enforcement agencies when necessary to secure the return of a consumer who is on an unauthorized leave of absence from any agency where the consumer was undergoing evaluation and treatment. EHN Associates will limit the information provided to name, address, date and place of birth, Social Security number, ABO blood type and Rh factor, type of injury, date and time of treatment, date and time of death (if applicable), and a description of distinguishing physical characteristics (such as height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos). If governmental or law enforcement officials need additional health information, EHN Associates will consult with the Legal Office before disclosing any additional information.
- EHN Associates may disclose this information to family members actively participating in the consumer's care, treatment, or supervision, but only if a mental health professional or other professional interviews the consumer and determines the release of information is in the best interest of the consumer. If the mental health professional or professional documents in the record that release is in the best interest of the consumer, EHN Associates will release only information relating to the person's diagnosis, prognosis, need for hospitalization, anticipated length of stay, discharge plan, medication, medication side effects, and short- and long-term treatment goals.
- EHN Associates may release information to a state agency that licenses health professionals and requires records during investigating complaints or negligence or incompetence, such as the Texas Medical Board, except that pursuant to 45 C.F.R. 164.512(d) (2), EHN will not release information where the consumer for whom records are requested is the subject of the investigation.
- EHN Associates may release information to local or state education official for a consumer between the age of three (3) and twenty-two (22) years, where the agency represents the information is necessary to provide educational services to persons with

disabilities. The information provided will be limited to evaluation and treatment information affecting the educational programming and placement decisions for the consumer and will be made only with the authorization of the consumer or consumer's representative.

- EHN Associates will release this information to a governmental agency or a competent professional as necessary to comply with state statutes concerning sexually violent persons.
- EHN Associates will release this information to human rights committees, only with the authorization of the consumer or consumer's representative.
- EHN Associates will not make any use or disclosure other than that listed in this policy without first consulting with the Compliance Office.

**Verification of Identity and Authority**

EHN Associates will verify the identity and authority of the recipient of the PHI.

**Disclosing the Minimum Necessary Amount of PHI**

EHN Associates will disclose only the minimum amount of PHI necessary for the purpose.

## 1.16 Consent for Uses and Disclosures Permitted

Emergence Health Network uses and discloses protected health information for treatment, payment, and health care operations as specified without consumer consent. The final Privacy Rule does not require covered entities to obtain consent for treatment, payment, and health care operations and makes consent optional. Due to no benefits in obtaining consent Emergence Health Network does not require consumers to consent for uses and disclosures for treatment, payment, and health care operations. Providing the option to consent gives consumers the right to revoke their consent at any time a consumer requests it. Revoked consents of uses and disclosure for treatment, payment, and health care operations will restrict Emergence Health Network from using and disclosing protected health information for those intended purposes.

**Procedure**

At the time of consumer's, authorized personal representative, or a child's first visit to the organization consumers will be given the notice of privacy practices. The notice shall contain all permitted uses and disclosures that may be made without the consumer's authorization. Review section 1.17 for additional details on use and disclosure of protected health information for treatment purposes. Review section 1.18 for additional details on use and disclosure of protected health information for payment purposes. Review sections 1.19 for additional details on use and disclosure of protected health information for health care operations. Consumers will not be given the option to consent for treatment, payment, or health care operations. Authorization for disclosures is required for any other types of disclosure not covered by treatment, payment, or health care operations.

## 1.17 Use and Disclosure of Protected Health Information for Treatment Purposes

Emergence Health Network uses protected health information pursuant to its notice of privacy practices and under the guidance of the HIPAA privacy

regulations for purposes of consumer treatment and care coordination. The use and disclosure of information for the purpose of treatment does not require specific authorization (see **section 1.33 authorization of use and disclosure**), this applies to a consumer, an authorized personal representative, or a child.

### **Procedure**

The use of information for treatment purposes is described in the notice of privacy practices. Before nonemergency treatment is initiated, an effort must be made to obtain the consumer's written acknowledgment of having received the notice of privacy practices. Obtaining the written acknowledgment is the responsibility of the assigned Emergence Health Network associate. If the consumer's acknowledgment cannot be obtained, the attempt to obtain an acknowledgment should be documented in writing.

Procedures for obtaining the acknowledgment are described in **section 1.31 notice of privacy practices**.

#### **1.17.1 Sharing of PHI for Treatment Purposes**

When a provider who is not a member of the practice contacts an EHN Associate and requests information for the purpose of treating a consumer previously treated at Emergence Health Network, the Associates may provide information without appropriate authorization. It is not necessary for the consumer to authorize the disclosure of protected health information that will be used for the purpose of treatment or an emergency.

When disclosing information to another provider for purposes of payment, Associates should use the following procedure.

- A consumer may have requested and been granted restrictions on the use or disclosure of protected health information. Associates should review the consumer's records to determine if any restrictions have been placed on the use or disclosure of protected health information.
- Before disclosing information for treatment purposes, an EHN Associate must verify the identity of the person making the request. In other words, the Associate must determine that the person making the request is, in fact, a health care professional who is requesting the information for the purpose of treatment. If the professional is known to the practice; is a member of a group that is known to an Associate; or is affiliated with a facility that is known to the practice; an Associate may presume that the provider is who he or she claims to be. Otherwise, an Associate should obtain additional assurances sufficient to satisfy his or her professional judgment that the person requesting the information is a health care provider who will use the information for purposes of treatment.

**If the request is made in person**, verification of identity may be accomplished by asking for photo identification (such as a driver's license or agency identification badge).

**If the request is made over the telephone**, verification may be accomplished by requesting identifying information such as birth date,

address, and/or medical record number and confirming that this information matches what is in the consumer's record. (The last four digits of the consumer's social security number (SSN) may be used as a last resort.) Or, verification will occur through a call-back process using phone numbers documented in the consumer record to validate the caller's identity or the main number of a business posted on their website or other public media source (Associates should not take a call back number from the person making the request over the telephone and notify the person that the associate will provide the information by calling the main number).

**If the request is made in writing**, verification may be accomplished by requesting a photocopy of photo identification. If a photocopy of the ID is not available, the signature on the written request must be compared with the signature in the Medical Record. In addition, associates may need to verify the validity of the written request by contacting the consumer by telephone.

- Protected health information should be sent only to the verified business address or phone number of the provider requesting it.

When an Associate requires information on a consumer's health condition from another provider, he or she may request the information without restriction. The consumer need not authorize this request.

The information requested must, however, be used for evaluating the consumer's medical condition or determining a course of treatment. A consumer may have requested and been granted a restriction on the information that is to be used or disclosed to other providers. In this situation, the restriction must be honored.

## 1.18 Use and Disclosure of Protected Health Information for Payment Purposes

Emergence Health Network uses protected consumer information pursuant to its notice of privacy practices and under the guidance of the HIPAA privacy regulations for payment purposes. The use and disclosure of information for payment purposes does not require specific authorization, but only the minimum necessary amount of information must be made available.

### **Procedure**

Use and disclosure of protected health information is permitted under this procedure to conduct the following activities:

- Providing information to the consumer's health plan to determine the consumer's eligibility for benefits and coverage
- Submitting a claim for services to the consumer's health plan
- Processing credit card transactions or transactions to obtain authorization for personal checks
- Providing information needed by the consumer's health plan to determine coverage, including information needed by the health plan to conduct medical review

Before seeking payment for nonemergency treatment, a consumer must be given the notice of privacy practices, and a written acknowledgment of receipt must be obtained. Obtaining the acknowledgment is the responsibility of the assigned EHN associate.

Procedures for obtaining an acknowledgment are described in **section 1.31**.

Use and disclosure of protected health information for payment purposes is limited to the information that can be transmitted using the standards for electronic transactions. These restrictions apply whether the transaction is conducted electronically or using paper forms.

## 1.19 Use and Disclosure of Protected Health Information for Health Care Operations

Emergence Health Network uses protected consumer information pursuant to its notice of privacy practices and under the guidance of the HIPAA privacy regulations for purposes of health care operations. The use and disclosure of information for health care operations-related activity does not require specific authorization, but only the minimum necessary amount of information must be made available.

### **Procedure**

Use and disclosure of protected health information is permitted under this procedure to conduct the following activities:

- Quality assessment and improvement
- Professional credentialing
- Medical and utilization review
- Legal services
- Auditing
- Business planning and market research
- Grievance procedures
- Due diligence analysis related to sales and acquisitions
- Creation of de-identified information and limited data sets
- Customer service
- Compilation of consumer directories
- Compliance monitoring
- Health information exchange sharing

Before using or disclosing protected health information for any of the functions included in health care operations, EHN must give the consumer its notice of privacy practices.

Obtaining an acknowledgment of receipt of the notice is the responsibility of the assigned EHN associate at each program. Procedures for obtaining an acknowledgment are established in **section 1.31**.

## 1.20 Use and Disclosure of Protected Health Information for Health Oversight Activities

EHN may disclose Protected Health Information (PHI) in response to certain legal requests without obtaining authorization from the consumer.

EHN shall ensure all disclosures of PHI requested for health oversight purposes comply with established procedures designed to protect and limit the amount of information disclosed.

### **Procedure**

EHN may disclose PHI to a health oversight agency for oversight activities authorized by law, including audits, civil, criminal, or administrative investigations, inspections, licensure or disciplinary actions, or other activities necessary for appropriate oversight of:

- The health care system;
- Government programs for which health information is necessary to determine eligibility for benefits;
- Entities subject to government regulatory programs for which health information is necessary to determine compliance with program standards; or
- Entities subject to civil rights laws for which health information is necessary to determine compliance with those laws.

In cases where a consumer is the subject of the investigation or other activity, EHN will not disclose PHI without authorization of the consumer unless the investigation, or other activity, arises out of and is directly related to:

- The receipt of health care;
- A claim for public benefits related to health; or
- Qualification for, or receipt of, public benefits or services when the consumer's health is integral to the claim for public benefits or services.

EHN may disclose PHI for public health purposes without authorization to a person or entity subject to FDA jurisdiction. The request must be related to the quality, safety, or effectiveness of an FDA-regulated product or activity for which that person has responsibility. Examples include:

- Collecting or reporting adverse events (or similar reports with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;
- Tracking FDA-regulated products;
- Enabling product recalls, repairs, or replacement (including locating and notifying individuals who have received products that have been recalled, withdrawn, or have other problems); or

- Conducting post-marketing surveillance.

EHN must limit its disclosure of PHI to the minimum necessary to meet the requirements of the law pursuant to which the request is made.

If a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits unrelated to health, EHN will consider the joint activity or investigation to be a health oversight activity.

EHN associates who receive a request for PHI for health oversight purposes should forward the request to the Administrative Director of Health Information.

Administrative Director of Health Information will: (1) verify the identity of the requestor; (2) ensure the request for records complies with applicable regulations; and (3) notify the originator of the request if the subpoena or request for records does not comply with applicable regulations.

For an FDA-related investigation, EHN Associates may identify the entity or entities responsible from the product label, written material that accompanies the product, or from sources of labeling, such as the Physicians' Desk Reference.

Documentation: EHN Associates must appropriately document the request and delivery of the PHI, including the name/identity of the requestor, the consumer whose PHI was disclosed, the EHN Associates who made the disclosure, the nature of the information disclosed and the date of the disclosure. This documentation should be made in the consumer's medical record.

## 1.21 Disclosures of Protected Health Information Relating to Judicial and Administrative Proceedings

EHN may disclose PHI in response to certain legal requests without obtaining authorization from the consumer.

EHN shall ensure all disclosures of PHI requested in litigation or administrative proceedings comply with established procedures designed to protect and limit the amount of information disclosed.

### 1.21.1 Qualified Protective Order

Qualified Protective Order means either: an order of a court or administrative tribunal or a stipulation of the parties to the underlying proceeding, which:

- Prohibits the parties to the underlying proceeding from using or disclosing PHI for any purpose other than the litigation or proceeding for which such information was requested; and
- Requires that, at the end of the litigation, the PHI is either destroyed or returned to EHN.

Reasonable efforts to secure a Qualified Protective Order means EHN receives a written statement and accompanying documentation (such as a copy of the order or stipulation) demonstrating that:

- The parties to the underlying dispute have agreed to a Qualified Protective Order and have presented it to the court or administrative tribunal; or

- The requesting party has requested a Qualified Protective Order from the court or administrative tribunal.

Reasonable efforts to notify the consumers whose PHI is being sought means EHN receives a written statement and accompanying documentation (such as a copy of the notice used) demonstrating that:

- The requesting party has made a good faith effort to provide a written notice of the request to the persons whose PHI is being requested, including sufficient information regarding the underlying litigation or proceeding to permit the persons to raise objections before the court or administrative tribunal; and
- The time for the persons whose information is being requested to raise objections has elapsed and no objections were filed, or the objections have been resolved such that the disclosure is permitted.

If the requesting party provides satisfactory assurance through the notification process, it is not the responsibility of EHN to respond to any objections from consumers who receive the notice or to explain the procedures by which to object, unless otherwise required by law.

### **Procedure**

EHN may disclose PHI in response to a court or tribunal order. If EHN makes a disclosure for this purpose, it may only disclose that PHI which is expressly authorized by the order.

In the absence of a court order, EHN may disclose PHI in response to a subpoena, discovery request, or other lawful process. If on the face of the subpoena it meets the requirements such as by demonstrating that the individual whose protected health information is requested is a party to the litigation, notice of the request has been provided to the individual or his or her attorney, and the time for the individual to raise objections has elapsed and no objections were filed or all objections filed have been resolved, no additional documentation is required. If EHN makes a disclosure for this purpose, it must receive "satisfactory assurance" that the requesting party has made reasonable efforts either to:

- Secure a qualified protective order; or
- Notify the consumer(s) whose PHI is being sought.

If EHN does not receive the required satisfactory assurance, it may not disclose the PHI, except that if EHN chooses, it may make its own efforts to respond and provide notice to the individual or seek a Qualified Protective Order.

In responding to the request, EHN must disclose only the minimum amount of information necessary to comply with its terms.

EHN Associates who receive a request for PHI through a court order, grand jury subpoena, or for law enforcement purposes should contact the Administrative Director of Health Information.

Once the Privacy Officer has determined a use or disclosure is lawful and appropriate under this Policy and Procedure, EHN associates should verify the identity and authority of the individuals requesting the PHI.

Once the identity and authority of the requestor has been verified, authorized EHN associates may access the consumer's PHI and make the disclosure.

Documentation: EHN Associates must appropriately document the request and delivery of the PHI, including the name/identity of the requestor, the consumer whose PHI was disclosed, the EHN Associates who made the disclosure, the nature of the information disclosed, and the date of the disclosure. This documentation should be made in the consumer's medical record.

## 1.22 Use and Disclosure for Specialized Government and Law Enforcement Officials

Emergence Health Network may use and disclose protected health information without written consumer authorization for certain legal requests or specialized government functions as described below. These specialized government functions are:

- Certain military and veterans activities, as required by the federal government
- National security and intelligence activities
- Protective service for the President of the United States and others as authorized by law
- Certain medical suitability determinations
- A correctional institution or other law enforcement custodial situation
- Government programs providing and/or administering public health benefits

### 1.22.1 Use and Disclosure for Military, Government, Law Enforcement, and Judicial Purposes

#### **Procedure**

Emergence Health Network may use and disclose information as appropriate to support military missions if appropriately directed by federal government agencies.

Emergence Health Network may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counterintelligence, and other national security activities authorized by law.

EHN shall ensure all disclosures of PHI requested for law enforcement purposes comply with established procedures designed to protect and limit the amount of information disclosed.

Emergence Health Network Associates may disclose protected health information requested by law enforcement agencies without obtaining the consumer's authorization.

EHN may disclose PHI (requested for a law enforcement purpose) to a law enforcement official as described in a court order or court-ordered warrant. All subpoenas, administrative requests, summons, and civil authorized investigative demand shall follow the EHN Policy relating to Disclosures of PHI Relating to Judicial and Administrative Proceedings Policy or contact the Administrative Director of Health Information.

EHN may disclose PHI in response to a law enforcement official's request for such information for identifying or locating a suspect, fugitive, material witness, or missing person.

- EHN Associates may report certain wounds and physical injuries to the Department of Family Protective Services [Adult Protective Services (APS) and/or Child Protective Services (CPS)] as required by state law.
- EHN Associates may report the name and address, date and place of birth, Social Security number, ABO blood type and Rh factor, type of injury, date and time of treatment or death, and a description of physical characteristics (height, weight, gender, race, hair and eye color, presence or absence of facial hair, beard or moustache, scars, and tattoos; and photograph of consumer if available) when requested by a law enforcement official.
- Associates may not report other information such as information related to DNA or DNA analysis, dental records, tissue typing, samples, or the analysis of body fluids or tissues without a court order, subpoena, or summons.

EHN Associates may report protected health information concerning the victim of a crime, but only with the agreement of the victim if victim is capable or when a law enforcement office indicates that the information is needed to investigate suspected criminal activity.

If EHN is unable to obtain the consumer's agreement because of incapacity or other emergency circumstance, EHN may disclose PHI if EHN obtains representations from the requesting law enforcement official that:

- Such information is needed to determine whether a violation of law by a person other than the victim occurred, and such information is not intended to be used against the victim; and
- Immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the consumer is able to agree to the disclosure; and
- EHN makes a determination, in the exercise of professional judgment, which the disclosure is in the best interests of the consumer.

Requests for disclosures made for the purposes of this section must be submitted by an authorized law enforcement official.

EHN may disclose PHI about a consumer who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the consumer if EHN has a suspicion that the death may have resulted from criminal conduct.

EHN may disclose PHI to a law enforcement official if EHN believes, in good faith, the information constitutes evidence of criminal conduct that occurred on the premises of EHN.

EHN may disclose PHI to a law enforcement official to report a crime in an emergency situation.

EHN may make a disclosure for this purpose if the disclosure appears necessary to alert law enforcement to:

- The commission and nature of a crime;
- The location of a crime or the victim(s) of the crime; or
- The identity, description, and location of the perpetrator of the crime.
- EHN Associates may report protected health information that is evidence of

criminal conduct on the premises of the practice.

EHN Associates should refer requests for protected health information received from law enforcement agencies to the Administrative Director of Health Information. The Administrative Director of Health Information will review requests for protected health information and obtain a legal opinion if he or she believes one is necessary before approving the disclosure of the requested information.

In regard to a judicial or legal action, EHN Associates may disclose protected health information only when such information does not contain references to alcohol or substance abuse in the following circumstances:

- The information has been requested by means of a subpoena accompanied by a valid consent for release or satisfactory assurance as stated below.
- The party seeking the protected health information has made a good-faith effort to provide a written notice to the subject of the request, has provided sufficient information to the subject of the request to permit the individual to object to the disclosure, and has resolved any objections that may have been raised or;
- The party seeking the protected health information provides written documentation that it has entered into or otherwise obtained a qualified protective order that a) prevents the parties to the legal action from using or disclosing protected health information for any purpose not related to the litigation or legal proceeding for which the information was requested, and b) requires the return or destruction of the protected health information at the conclusion of that proceeding.
- The information has been requested in a court order or an order of an administrative tribunal.
- The information has been requested by means of a subpoena, discovery request, or other legal process accompanied by a court order.
- The information has been requested by means of a grand jury subpoena.

If protected health information contains references to alcohol or substance abuse treatment such information must be redacted unless a valid consent for release of this information is on file or otherwise a valid court order pursuant to 42 CFR Part 2 has been presented. Any release of this information shall be accompanied by the requisite language specified under 42 CFR Part 2 included in Appendix A.

Before responding to the request, efforts should be made to ensure that disclosure is limited to the minimum protected health information specifically requested.

Except when a request is accompanied by a valid authorization for release, EHN Associates should refer requests for protected health information to the Medical Records Supervisor. The Medical Records Supervisor will notify and seek guidance from legal counsel on how to respond to the request. Before responding, the Medical Records Supervisor will obtain the assurances described in this procedure.

### 1.22.2 Use and Disclosure for Public Health

## **Procedure**

The following information may be reported to Department of State Health Services, Department of Aging and Disability Services, Department of Assistive and Rehabilitative Services, Health and Human Services as required by law whether or not the consumer authorizes the disclosure:

- Information required to compile vital statistics (births and deaths)
- Information on reportable injuries

Associates may disclose protected health information to government agencies such as the Department of State Health Services, Department of Aging and Disability Services, Department of Assistive and Rehabilitative Services, which are responsible for administering public health programs such as Medicare and Medicaid, and for licensing providers, conducting audits, and for other purposes related to the oversight of the health system.

- EHN Associates should refer requests for protected health information received from oversight agencies to Medical Records Supervisor.
- The Medical Records Supervisor will review requests for protected health information and obtain a legal opinion if he or she believes one is necessary before approving the disclosure of the requested information.

## **1.23 Disclosures of Protected Health Information Relating to Communicable Diseases**

### **Procedure**

#### Special Confidentiality Treatment

- EHN Associates will maintain the confidentiality of communicable disease-related information (including AIDS and HIV-related information) and will disclose that information only in compliance with this policy.
- EHN policies on the use and disclosure of PHI do not apply to communicable disease-related information unless otherwise noted.

### **1.23.1 Disclosure of Communicable Disease-Related Information (Including HIV-Related Information) without Consumer Authorization**

If a person or entity is not listed below, EHN Associates will obtain consumer authorization under the (Reporting of Communicable Diseases) paragraph before disclosing the information.

- **Consumer or Consumer's Legal Representative:** EHN Associates may disclose communicable disease-related PHI to the consumer or the consumer's representative.
- **Other Health Care Providers:** EHN Associates may disclose communicable disease-related PHI to another health care facility or provider if the disclosure is necessary to provide appropriate care to the consumer or the consumer's child. Before sending the PHI, EHN Associates will confirm with the receiving facility or provider that their employees or agents receiving the PHI have authorized access to medical records for purposes such as provision of health care, records maintenance, or billing.

- Organ Procurement for Medical Education, Therapy or Transplantation: EHN Associates may disclose communicable disease-related PHI to a health care provider or facility for procurement, processing, distributing, or using a human body or body parts for use in medical education, therapy, or transplantation.
- Quality Review and Oversight
  - EHN Associates may use or disclose confidential communicable disease-related PHI to organizations, committees or individuals engaged by EHN to review professional practices at EHN (such as peer review, utilization review, medical necessity committees, The Joint Commission, other oversight, or accreditation agencies).
  - The disclosure must be limited to that information necessary for the authorized review and may not include information “directly” identifying the consumer, such as name, Social Security number, phone number or address.
- Government Officials
  - EHN Associates will disclose communicable disease-related information to local, county, state, and federal health officers when required by federal or state law to do so.
  - EHN Associates will follow EHN policies and procedures concerning communicable disease reporting obligations.
  - EHN Associates may disclose communicable disease-related information to federal or state officials who oversee EHN, such as the state Department of Health Services and the Federal Centers for Medicare and Medicaid Services. Communicable disease-related PHI released for this purpose may not include the consumer’s name.
- Court or Administrative Order or Search Warrant
  - EHN Associates may release confidential communicable disease-related PHI to a person designated in a valid court or administrative order or search warrant.
  - The court or agency may issue the order or search warrant only if:
    - There is a compelling need for the information in a court or administrative proceeding;
    - A person is in clear and imminent danger of exposure;
    - There is a clear and imminent danger to public health;
    - The person requesting the information is lawfully entitled to the information; or
    - There exists either a clear and imminent danger to a person or to public health or there is a compelling need to disclose the information.
  - If there is any doubt or question regarding the sufficiency of the legal order seeking disclosure, EHN Associates should obtain advice from EHN legal counsel before making the disclosure.
  - Workers’ Compensation Claims: If communicable disease-related PHI is pertinent to a workers’ compensation claim, EHN Associates may disclose requested PHI to the Industrial Commission or parties to an Industrial Commission claim.

- Cause of Death: EHN Associates may list communicable disease-related illnesses on a death certificate or autopsy report to document the cause of death.

### 1.23.2 Disclosure of Communicable Disease-Related Information (Including HIV-Related Information) with Consumer Authorization

- If a disclosure is not permitted under the Disclosure of Communicable Disease-Related Information (Including HIV-Related Information) without Consumer Authorization paragraph above, EHN Associates will obtain consumer authorization before disclosing communicable disease-related PHI.
  - The authorization will meet the requirements of the EHN authorization policy.
  - If EHN Associates seek to disclose HIV/AIDS-related information, the authorization form must specifically indicate its purpose to authorize disclosure of HIV-related information.
- When EHN Associates make any disclosure of communicable disease-related PHI with consumer authorization, they will prepare a written statement that will accompany the production of the PHI warning the information is confidential and protected by state law that prohibits further disclosure without specific written authorization by the consumer.

### 1.23.3 Disclosures to Persons Exposed to Communicable Diseases

- Except as provided below, EHN Associates will not communicate directly with a person who has been exposed to a communicable disease by a consumer. Rather, EHN Associates will report the exposure to the appropriate state department of health, following the EHN policies and procedures on communicable disease reporting obligations.
- If an EHN mental health professional knows or has reason to believe that a significant exposure has occurred between a consumer and EHN Associates (or other health care or public safety) employee, the mental health professional may consult with the consumer and ask the consumer to release the information voluntarily.
- If the consumer refuses to release the information concerning the significant exposure, the mental health professional may report directly to the exposed employee of the possibility of the communicable disease or HIV-related exposure in a manner that does not identify the consumer.

### 1.23.4 Record and Accounting of Disclosures

- EHN Associates making a disclosure of communicable disease-related PHI will keep a written record of all disclosures.
- On request, EHN will give the consumer or his or her personal representative access to the record of disclosures

### 1.23.5 HIV-related testing

- EHN Associates ordering an HIV-related test must obtain the consumer's explicit permission to do so using the EHN written, informed consent for HIV testing.
- Oral consent is required if the test is done anonymously.

### 1.23.6 Verification of Identity and Authority of PHI Recipient

EHN Associates will verify the identity and authority of the recipient of the PHI.

### 1.23.7 Disclosing the Minimum Necessary Amount of PHI

EHN Associates will disclose only the minimum amount of PHI necessary for the purpose.

## 1.24 Use or Disclosure of Sale of Protected Health Information

In order to use or disclose a consumer's PHI in exchange for direct or indirect remuneration from or on behalf of the recipient of the information, EHN must obtain an authorization for any disclosure. The authorization must state the disclosure will result in remuneration to the Covered Entity. Sale of PHI is prohibited without a consumer's authorization.

If EHN is the recipient of the PHI, EHN cannot re-disclose the PHI in exchange for remuneration unless a valid authorization is obtained.

### 1.24.1 Guidelines:

- The sale of PHI does not include payments EHN may receive in the form of grants, contracts, or other arrangements to perform programs or activities, such as a research study. EHN may receive only a reasonable, cost-based fee to cover the cost to prepare and transmit the information for research purposes.
- Remuneration, as applied to the sale provisions, is not limited to financial payment in the same way it is limited in the marketing provisions.
- The provisions prohibit the receipt of remuneration not only from the third party that receives the PHI, but also from another party on behalf of the recipient of the PHI.
- The sale provisions apply to disclosures in exchange for remuneration including those that are the result of access, license, or lease agreements.
- Exceptions:
  - EHN may receive remuneration for use or disclosure of PHI for public health activities and/or for treatment and payment purposes.
  - EHN may disclose PHI related to the sale, transfer, merger, or consolidation of all or part of it.
  - EHN may disclose PHI to an individual for providing a right to access PHI or providing a right to receive an accounting of disclosures.

EHN may disclose PHI as required by law.

- If EHN is a Business Associate, the following guidelines apply:
  - EHN may disclose PHI for activities undertaken on behalf of a Covered Entity, as long as the only remuneration provided is by the Covered Entity to the Business Associate for the performance of such activities; and
  - As long as EHN is performing the activities pursuant to a Business Associate contract.

- The exceptions in Paragraph above does not apply if EHN receives remuneration above the actual cost incurred to prepare, produce, and transmit the PHI for the permitted purpose, unless such fee is expressly permitted by other law.

### **Procedure**

EHN must obtain an authorization for any use or disclosure for the sale of a consumer's PHI.

EHN must obtain consumer authorization on the EHN Release of Information form that contains the following items:

- A specific and meaningful description of the PHI to be used or disclosed;
- The name of the person, class of persons, or organization that will be making the disclosure of PHI, *e.g.*, EHN;
- The name or other identification of the person, class of persons, or organization to whom EHN is making the disclosure;
- Specifically state the PHI is to be sold and EHN will receive remuneration;
- An expiration date or an expiration event of the authorization that relates to the purpose of the use or disclosure;
- A statement that the consumer has a right to revoke the authorization, and a reference to EHN's Notice of Privacy Practices for details on that right;
- A statement that EHN cannot condition treatment on whether the consumer signs the authorization;
- The consumer's (or personal representative's) printed name, signature, and date of signature;
- If the authorization is executed by a personal representative, a description of that person's authority to act for the consumer; and
- A statement that EHN will receive either direct or indirect payment.

## **1.25 Use and Disclosure for Marketing and Fundraising**

Emergence Health Network may not inappropriately use protected consumer information for marketing or fundraising and will provide all consumers an ability to opt out of all marketing and fundraising communications.

### **1.25.1 Use and Disclosure for Marketing**

#### **Procedure**

The following types of marketing communications do not require authorization:

- Communications to members of health plans that describe EHN, its members, and the services that are available from the practice, unless financial remuneration is provided to the practice for the communication
- Communications to a consumer as part of the consumer's treatment that are specific to the medical condition of the consumer, unless financial remuneration is

provided to the practice for the communication

- Communications from the consumer's health plan during treatment for the purpose of alerting the consumer to the availability of alternative treatments, therapies, health care providers, or treatment settings, unless financial remuneration is provided to the practice for the communication
- Face-to-face communications between EHN Associates and consumers during a consumer visit
- Promotional gifts of nominal value such as pens, note pads, or coffee mugs

Consumers must specifically authorize the use of protected health information collected or maintained by EHN for a communication that is sent to the individual describing a product or service offered by an organization other than EHN. Examples include mailings by pharmaceutical companies, retail pharmacies, health clubs, and suppliers of unrelated medical services such as durable medical equipment. Also, any communications that involve direct or indirect remuneration to the provider require authorization from the consumer, even if they are describing a health-related product or service provided by the organization itself.

### 1.25.2 Use and Disclosure for Fundraising

#### **Procedure**

The following information may be used by EHN, and/or disclosed to a business associate, to support fundraising efforts by the covered entities without the consumer's authorization:

- Demographic information describing the individual (i.e., name, date of birth, sex, address, and other nonclinical information that describes the consumer)
- The dates on which the consumer received health care services from EHN
- Department in which the service was provided
- The treating mental health professional- a qualified individual with training or state issued license to deliver psychological assessments, therapy, diagnosis, medication, skills training and/or rehabilitation services.
- Information about consumer outcome
- Health insurance status

Other protected health information may not be used in fundraising activities without the consumer's authorization. That is, the consumer's authorization is required for the use of any protected health information except those items found in the list above.

Fundraising appeals sent to individuals must include the following paragraph describing how the individual may opt out of further fundraising communications:

To be removed from future fundraising appeals, please call 915-887-3410 and ask to be removed from our fundraising mailing list, or check off the box asking to be removed from our fundraising mailing list on the reply card and return it to the office by dropping it in a mailbox.

A fundraising mailing list will be maintained by the Director of Communications. When a consumer asks to be removed from the mailing list, no additional

fundraising communications may be sent to this consumer.

Protected health information may not be used to support fundraising on behalf of other organizations (that is, for raising funds that do not benefit the practice directly) without the consumer's authorization.

## 1.26 Use and Disclosures for Facility Directories

Emergence Health Network will provide patients with the opportunity to agree to or prohibit the use and disclosure of their protected health information for programs that have a facility directory (in patient programs).

### **Procedure**

The patient or personal representative must be given an opportunity to object orally or in writing to being listed in the directory at the time of admission or service.

EHN must take the following steps before including any of a patient's protected health information in the directory:

Inform the patient of EHN's policies regarding its directory, if any; and

Provide the patient with an opportunity to not be included in the directory listing or to restrict some or all of their protected health information that EHN desires to include in the directory.

If a patient does not orally or in writing object to his or her PHI being listed in the directory, the facility may include the following PHI in its facility directory:

- The patient's name;
- The patient's location in the facility;
- The patient's condition described in general terms that do not communicate specific medical information about the individual (e.g., "fair", "good", "critical", etc.);
- The patient's religious affiliation;

If a patient does not orally or in writing object to his or her PHI being listed in the directory, the facility may disclose for directory purposes such information:

- To members of the clergy and
- Except for religious affiliation information, to persons other than members of the clergy who ask for the patient by name;

The information described above may be disclosed to members of the clergy whether or not the clergy asks for the patient by name. In addition, the patient's religion may be made available to members of the clergy.

Emergency Situations:

Emergency situations may arise in which the patient is not able to be given the opportunity to object to being listed in the directory.

If the opportunity to object to being listed in the directory cannot practicably be provided because of the patient's incapacity or an emergency treatment circumstance, EHN may list the patient in the facility's directory if the listing is:

- Consistent with a prior expressed preference of the patient, if any, known to EHN; and
- In the patient's best interest as determined by EHN in the exercise of professional judgment.

When it becomes practicable to do so, EHN must inform the patient of the PHI included in the directory, to whom such PHI may be disclosed, and must at that point provide the patient with an opportunity to object to being listed in the directory.

## 1.27 Other Uses and Disclosures of Protected Health Information

Emergence Health Network will make protected health information available as appropriate under the HIPAA privacy regulations.

### 1.27.1 Disclosure of Information for the Purpose of Cadaveric Organ Donation

#### **Procedure**

Following the death of a consumer, EHN may disclose protected health information to an organ procurement organization such as an eye bank or tissue bank without the consumer's prior authorization and without obtaining the authorization of the consumer's representative.

EHN Associates may not disclose this information if a consumer or the consumer's representative has indicated that he or she does not want to donate organs or tissue, or if the consumer has imposed a restriction on the disclosure of protected health information for this purpose.

### 1.27.2 Disclosure of Information to Coroners and Medical Examiners

#### **Procedure**

EHN Associates may disclose protected health information without the consumer's authorization to a coroner or medical examiner who requests the information for the following purposes:

- Identification of a deceased person
- Determination of the cause of death
- Other purposes specified in state or federal law

The credentials of the coroner or medical examiner making the request should be verified. If the request is made in person, associates should ask to be shown an official identification. If the request is made by telephone, associates should ask that the request be submitted in writing and should obtain the official address to which information should be sent.

EHN Associates should confirm that the information is being requested by the coroner or medical examiner to establish the identity of a deceased person or determine the cause of death.

The requested information should be sent only to the official address of the coroner or medical examiner.

### 1.27.3 Disclosure to Avert a Threat to Health or Safety

#### **Procedure**

An EHN Associate may disclose protected health information without the consumer's authorization if, in his or her professional judgment, such disclosure is necessary to reduce a serious and imminent threat to the health

and safety of a person or the public.

- Information may be disclosed only to a person who is able, in the Associates judgment, to prevent or lessen the threat.
- If the consumer has threatened to harm or injure another person or persons, that threat may be disclosed to the person(s) identified by the consumer as the target(s).
- If the consumer has admitted that he or she has participated in a violent crime, that admission may be disclosed to law enforcement agencies.
- If an EHN Associate has reason to believe, based on all circumstances, which the consumer has escaped from a correctional facility or other form of custody, Associates may disclose that belief to law enforcement agencies.

EHN Associates may not disclose information related to participation in a violent crime if that information is learned in the course of treatment, counseling, or therapy for a propensity to engage in the criminal conduct, or if the consumer has disclosed criminal activity while requesting referral for treatment, counseling, or therapy of such a propensity.

#### 1.27.4 Disclosure to Disaster Relief Agencies

##### **Procedure**

Information on a consumer's location, medical condition, or death may be disclosed to disaster relief organizations such as the Red Cross and other public or private organizations.

#### 1.27.5 Disclosure for Purposes of Research

##### **Procedure**

Use and disclosure of information for purposes of research is allowable under the rule with authorization from the consumer. In some instances, it is also allowable without specific signed authorization.

Authorization for disclosures must ensure that the consumer is aware in writing of the potential for future research purposes of their collected information. The authorization must be in plain language and contains specific information. The following items must be included in the authorization:

- Authorizations for disclosure of protected health information must include a "description of each purpose of the requested disclosures or the statement" *at the request of the consumer*" this is a sufficient description of the purpose when a consumer does not provide a statement for each purpose for disclosures.
- Authorizations do not need to specify each specific study if the studies to be conducted are not yet determined. The authorizations must adequately describe such purposes such that it would be reasonable for the consumer to expect that "*his or her protected health information could be disclosed for such future research*". If there are specific research studies planned in the future the authorization could be specific for those studies.
- Authorizations for disclosures of protected health information for future research must contain "an expiration date" or an expiration event that

relates to the consumer or the purpose of the disclosure such as “that the authorization will remain valid unless and until it is revoked by the consumer”.

- Authorization must inform the consumer of the right to revoke the authorization in writing, “the exceptions to the right to revoke and a description of how the individual may revoke their authorization”.

EHN may only use or disclose de-identified information for the purposes of research, public health, or health care operations or to a Business Associate who has submitted the appropriate documentation as required in EHN’s Business Associate Agreement.

All requests for de-identified information should be submitted to the Administrative Director of Health Information for review via the Research Request Application (see **Appendix A**). The Administrative Director of Health Information will review and forward the application for approval by leaders of the Division/Department that will be used for research purposes and other disciplines as necessary. Final approval will come from the Chief Executive Officer. The requestor will receive written approval to disclose EHN data.

EHN Associates may provide a researcher with protected health information in the following instances:

- With a signed authorization from the consumer (sometimes found within the informed consent form for the research study)
- With a HIPAA waiver from the applicable institutional review board or privacy board
- When a data use agreement is in place with the researcher and there is a limited data set provided to the researcher, as described in the data use agreement
- If the information has been de-identified

## 1.27.6 Disclosures to Schools Regarding Immunizations

### **Procedure**

Associates may disclose information regarding immunizations about a consumer who is a student or a prospective student at an educational institution, if those immunizations are required by the state or other law for admission. Certain requirements must be met in order to provide this information to the educational institution.

- A request must come from the educational institution or from the parent/guardian/consumer.
- The protected health information to be provided to the school is limited to the proof of the immunizations required.
- The school must be required by state or other law to have proof of these immunizations on file before admission of this student.
- The parent, guardian, or the individual himself (if he or she is of age or an

emancipated minor) must agree to the disclosure, and this must be documented by the practice.

### 1.27.7 Disclosure of Protected Health Information After Death

#### **Procedure**

The protected health information of a deceased individual is handled according to the policies and procedures applied to the protected health information of living consumers. The death of a consumer does not reduce the privacy protections that his or her protected health information will receive until 50 years after his or her death. At that point, health information is no longer considered protected health information unless specially protected by a law other than HIPAA.

### 1.27.8 Disclosures by Workforce Members Who Are Crime Victims

#### **Procedure**

Associates of Emergence Health Network may disclose protected health information to a law enforcement official provided that the information is about the suspected perpetrator of the crime and the associate is the victim of a crime. The information must be limited to name and address; date and place of birth; social security number; ABO blood type and rh factor; type of injury; date and time of treatment; date and time of death; if applicable; and a description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence of facial hair (beard or mustache), scars, and tattoos.

## 1.28 Communications and Media Relations

Emergence Health Network will ensure that all employees and associates who engage in communications and media relations activities on behalf of the organization do so in a manner compliant with the HIPAA privacy regulations and have approval from the Director of Communications.

#### **Procedure**

##### **Internal Uses of PHI**

Interviews with and/or articles about individuals circulated within Emergence Health Network— When writing articles or stories that are printed in publications circulated within Emergence Health Network, may contact the individual, or a health care provider to access the individual, to obtain signed consent from the individual allowing Emergence Health Network to interview him or her and to obtain information for the article or story.

Consumer satisfaction surveys—Quality assessment and improvement activities are considered health care operations under the privacy regulations. To conduct consumer satisfaction surveys, which are quality assessment and improvement activities, Emergence Health Network must state in its notice that it may use PHI for health care operations. If Emergence Health Network uses a vendor to conduct consumer satisfaction surveys on behalf of Emergence Health Network, there must be a business associate agreement in place.

##### **External Disclosures of PHI**

Media inquiries regarding an individual—Emergence Health Network facility

directories may contain the following information about an individual: (a) name, (b) location in the facility, (c) the condition of that individual in terms that do not communicate specific medical information (for example, critical, satisfactory, good). Emergence Health Network must give individuals the opportunity to restrict or prohibit the use or disclosure of PHI for facility directories and inform the individual that Emergence Health Network may disclose this information to the media.

Associates should not disclose if a consumer is receiving services through Emergence Health Network. Associates will first state that, *“they will need to verify the identity of the requestor before any information is disclosed and the associate will need to verify if the individual that is being inquired about is a client of Emergence Health Network.”*

The Associate will next search the electronic health record for the individual that is being inquired about and if found, review for Consent to Release Information has been authorized. If consent has been authorized only then can the associate disclose information to the media upon approval from their supervisor.

If the individual is incapacitated or deceased, or there is an emergency treatment situation, Emergence Health Network may use or disclose some or all of the PHI in the facility directory if such use or disclosure is consistent with a prior expressed preference or if such use or disclosure is considered in the best interest of the individual. Emergence Health Network must inform the individual of the use or disclosure when it is practical to do so.

When the media does not know an individual's name but give other identifying information such as location or address of an accident, Emergence Health Network may disclose non-consumer specific information, such as age and gender, in addition to the condition of the individual. If the media inquire about an individual by name, subject to that individual's objection, Emergence Health Network may give the media the information contained in the facility directory.

Media requests for interviews with and/or articles about an individual—Mental health professionals, other health care providers and/or media relations Associates who provide PHI about individuals to be included in an article or story must obtain the individual's written authorization before making such a disclosure.

Photographs, videotapes or other images of individuals—Emergence Health Network must obtain an individual's written authorization before photographing or videotaping that individual for medical education, staff education, or publicity purposes. If the individual's written authorization specifically allows the reuse of the information described above, the information may be reused in accordance with the authorization. If the authorization does not specifically allow the reuse of information, the information may not be reused.

## 1.29 Offshoring Information Outside the United States

Emergence Health Network will ensure that offshoring, the use, disclosure, creation, maintenance or transmission of confidential information outside of the United States is done under written permission per the HHS Data User Agreement.

### **Procedure**

Requests to release information to entities outside of the United States will not be processed until a complete review of the request has been completed and has been approved by the Chief Information Officer, Chief Compliance Officer, Chief Executive Officer, and Health and Human Services (HHS). Requests will be reviewed on a case by case basis to include any law violations regarding the offshoring of Medicaid programs, HHS contractual requirements and data use agreements regarding the securities of protected health information, (e.g. subcontracting with an entity outside of the United States to provide appointment reminder calls to clients).

## **1.30 Publishing Confidential Information**

Emergence Health Network will ensure that publishing confidential information, offshoring, the use, disclosure, creation, maintenance or transmission of confidential information outside of the United States is done under written permission per the HHS Data User Agreement.

### **Procedure**

Requests from entities to publicly release or publish protected health information will not be processed until a complete review of the request has been completed and has been approved by the Chief Information Officer, Chief Compliance Officer, Chief Executive Officer, and Health and Human Services (HHS). Requests will be reviewed on a case by case basis to include violations of HIPAA laws, 42 CFR Part 2, contractual agreements and data use agreement with Health and Human Services, (posting the names of clients on the company website or social media; using television, newspaper, or radio to communicate the story of a client without appropriate permission).

## **1.31 Notice of Privacy Practices**

Emergence Health Network is required to provide a notice of privacy practices to all consumers or any persons requesting a copy. All individuals have a right to receive adequate notice of the uses and disclosures of protected health information that may be made by an organization, and of the individual's rights and Emergence Health Network's responsibilities with respect to protected health information.

*Sample notices of privacy practices as well as a sample acknowledgment form are found in **Appendix A** in the back of this manual.*

### **Procedure**

The Administrative Director of Health Information is responsible for developing the notice of privacy practices.

The notice of privacy practices must be written in language that most consumers of average intelligence and education will be able to understand. The notice must contain the following elements.

The following language must appear exactly as it is shown here and must be prominently displayed at the top of the notice:

**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.

### **Uses and Disclosures**

This section of the notice must describe and give examples of the uses and disclosures for purposes of treatment, payment, and health care operations covered by the notice.

It must identify the legally mandated disclosures that may be made without the consumer's authorization.

It must indicate that any other use or disclosure of protected health information requires written authorization by the consumer, and that an authorization may be revoked by the consumer.

### **Additional Uses of Information**

The uses and disclosures listed in this section must be specified if EHN intends to use protected health information for any of the listed activities. This section can be merged with the previous section.

This section identifies any use of protected health information in the preparation of appointment reminders, in offering information about treatment and other health-related benefits or services, or to conduct fundraising for the practice.

### **Individual Rights**

This section of the notice of privacy practices must identify the rights of the consumer under the federal privacy rule. These must include:

- The right to request restrictions
- The right to receive confidential communication
- The right to inspect and copy protected health information
- The right to amend protected health information
- The right to receive an accounting of disclosures
- The right to receive a printed copy of the notice of privacy practices itself

### **Emergency Health Network's Duties**

This section describes the duties of the organization, specifically with respect to maintaining the privacy of protected health information, giving the notice of privacy practices to consumers, and abiding by the terms of that notice. Emergency Health Network will not use or share protected health information that is inconsistent with the privacy practices notice.

### **Right to Revise Privacy Practices**

The notice must clearly state that the organization reserves the right to modify its privacy practices and that should it do so, the revised notice will be made available to consumers upon their request.

### **Complaints**

This section must outline the procedure for submitting complaints concerning the organization's privacy practices or to report suspected violations of privacy rights.

It also must indicate that the organization will not retaliate against the consumer for submitting a complaint or reporting a suspected violation.

**Contact Person**

Administrative Director of Health Information/Privacy Officer  
PO Box 9997  
El Paso, TX, 79995-2997  
(915) 887-3410

**Effective Date**

This section must give the effective date of the notice of privacy practices. The effective date may not be earlier than the date on which the notice is printed and made available for distribution.

In the case of revisions to the notice, the effective date of the revised notice may not be earlier than the printing and release date of the revised notice. In other words, the policies described in the notice cannot go into effect before consumers have been informed of the policies.

**1.31.1 Giving the Notice of Privacy Practices to Consumers**

**Procedure**

The notice of privacy practices must be given to all consumers at the time of their first visit to the organization. The notice must also be given to any consumer who requests one at any time.

- All consumers will be given a copy of the notice during their first contact following April 14, 2003, whether in person in the office, via a telephone consultation or through other electronic means such as email.
- Any consumer who requests a copy of the notice will be given a copy.
- A copy of the notice will be posted in waiting areas. If EHN maintains a website, the notice will be posted on that site. An individual who receives a copy of the notice electronically (by email) also may request a printed copy of the notice.

**1.31.2 Acknowledgment of the Notice**

**Procedure**

All consumers must be asked to sign an acknowledgment that they have received a copy of the notice of privacy practices. If the consumer cannot sign the acknowledgment, his or her personal representative may sign the acknowledgment. If the consumer cannot sign the acknowledgment and a personal representative is not available or if the consumer refuses to sign the acknowledgment, the Associate who requests the acknowledgment must document the attempt to obtain an acknowledgment and briefly summarize the reason it was not obtained.

When a consumer requires emergency treatment, providing the notice and obtaining an acknowledgment should be delayed until the consumer's condition has been stabilized.

Copies of all signed acknowledgments should be included in the consumer's

medical record.

### 1.31.3 Notice of Substance Abuse Confidentiality

#### **Procedure**

At the time of admission associates shall communicate to any consumer receiving substance abuse or alcohol treatment that federal law and regulations protect the confidentiality of records for person's receiving substance abuse services. The persons shall be given a written summary of the federal law and regulations. A copy of the notice should be given to the person with the original filed in the person's record.

## 1.32 Verification of the Identity and Authority of a Consumer Requesting Disclosure of Protected Health Information

Members of the workforce who authorize the disclosure of PHI will take reasonable steps to:

- Verify the identity of the person to whom the PHI is disclosed.
- Verify the person's authority to receive the PHI.

Depending on the circumstance, verification prior to disclosure of PHI should include the following:

- If the employee knows the identity and authority of the recipient of the PHI firsthand, no further verification is necessary.
- PHI may be disclosed in accordance with EHN policies regarding disclosures to law enforcement officials, prison officials, or disaster relief agencies when the identity and authority of the recipient of the information may reasonably be inferred from the circumstances.
- PHI may be disclosed as required by a subpoena or other legal document if the document meets the provisions of existing policy in this area.
- Any legal documentation required by EHN policy, must be obtained before the PHI is disclosed.

EHN employees may rely on any of the following to verify the identity of a public official who requests PHI be disclosed without the consumer's authorization:

- An identification badge;
- Official credentials;
- Other proof of government status;
- Written request on the appropriate agency letterhead along with official identification; or
- Written evidence is required when a consumer is acting under government authority (such as a contract or purchase order that verifies a private citizen is acting as an agent of a government agency in requesting the PHI) along with identification.

EHN employees may rely on any of the following to establish the authority of a public official to receive PHI requested without the consumer's authorization:

- A written statement of legal authority to request the information;
- An oral statement of legal authority (if a written statement is impractical under the circumstances); or
- A legal process issued by a grand jury or a judicial or administrative tribunal.
- Verification of identification will be documented within the consumer record.

## 1.33 Authorization of Use or Disclosure

Emergence Health Network will use and disclose protected health information in certain situations only pursuant to a written, signed consumer authorization, as designated by the HIPAA privacy standards or other pertinent state laws.

*A sample Authorization of Use and Disclosure form is found in Appendix A in the back of this manual: Consent to Release Information.*

### **Procedure**

When an EHN Associate knows in advance of collecting or creating protected health information that the information will be used or disclosed for a purpose not covered by the notice, the Associates should seek the consumer's authorization at the time the information is collected.

It is not necessary, however, to obtain the consumer's authorization before the information is created. Authorization can be obtained at any time after it is created but before the information is used or disclosed for a purpose not covered by the notice.

EHN Associates who uses or discloses the information is responsible for obtaining the consumer's authorization. The consumer or the consumer's representative must be given a copy of the signed authorization.

- EHN Associates requesting the authorization should obtain an authorization form and complete the sections describing the information to be used or disclosed, the purposes of the use or disclosure, the persons who will use or disclose the information, and the persons to whom the information will be disclosed.
- EHN Associates or a person designated by the Associate should review the authorization request with the consumer.
- The consumer may request restrictions on the use and disclosure of protected health information. EHN Associates requesting the authorization should consider these requests and may, at his or her discretion, accept or reject them. Accepted restrictions should be clearly noted on the authorization form.
- The consumer should sign and date the authorization form.
- The signed and dated authorization form should be placed in the consumer's record.
- The consumer must be given a copy of the signed and dated authorization form.

### 1.33.1 Consumer's Refusal to Sign an Authorization Form

#### **Procedure**

A consumer who refuses to authorize a specific use or disclosure may not be refused treatment except under the following circumstances:

- The treatment is available only to participants in a research study. A consumer who does not authorize use of information for research may be refused treatment that is available only to participants in the research study.
- The services to be provided have no purpose other than responding to a request for information from another entity (for example, from a parent requesting a physical for a child who wants to participate in sports programs).

When a consumer refuses to sign an authorization, it should be determined whether the request involves information included in either of the two categories listed above.

If the authorization is for use and disclosure of information for purposes of research-related treatment, the consumer should be told that the treatment is available only to participants in a study and that participants must authorize use and disclosure of their information in the study.

If the authorization involves a request for information from another organization, the consumer should be told that the services will not be provided unless disclosure is authorized.

If the consumer continues to refuse to sign the authorization, the persons requiring the authorization should be notified of the consumer's refusal.

### 1.33.2 Revoking of an Authorization for Use or Disclosure

#### **Procedure**

Associates shall give full effect to any revocation by a consumer. A consumer may revoke an authorization in writing or verbally. The revocation should be noted in the file. EHN Associates should explain to the consumer that revoking the authorization will not affect any use or disclosure of information that has already occurred.

It is preferable that the Associates complete the revocation form in the EHR software. The consumer should sign and date the revocation form. The revocation form should be appended to the authorization and included in the consumer's records.

#### Authorized Employee

- Receives request from a consumer or personal representative to revoke an authorization.
- If the request is from someone other than the consumer, verify the individual has the authority to make the request.
- If the individual has the authority to make a request (consumer or personal representative), forward the request to Medical Records/Medical Records Supervisor for processing.

- If the individual does not have the authority to make the request:  
Notify the individual of the request denial; and  
Document the call.

#### Medical Records Supervisor

- Determine if the authorization can be revoked.
- If the authorization cannot be revoked as stated in the policy section above, send a letter to the consumer stating the reason for the denial.
- If the authorization can be revoked:  
Document the request; and  
Notify the appropriate associates to update appropriate systems.

## 1.34 Consumer Requests for Restrictions on Uses and Disclosures of Confidential Communications

Emergence Health Network recognizes the consumer's right to request restrictions on specific uses and disclosures of protected health information, as well as to request confidential communications in certain instances.

Consumers have a right to ask EHN to communicate with them about Protected Health Information (PHI) at alternative addresses or by alternative means ("confidential communications"). EHN will accommodate reasonable consumer requests. This policy provides a mechanism for handling consumer requests for these confidential communications.

### 1.34.1 Consumer Requests for Restrictions on Use and Disclosure

#### **Procedure**

A consumer may request restrictions on the use and disclosure of protected health information for treatment, payment, and health care operations as described in the notice of privacy practices. A consumer also may request restrictions on the use and disclosure of protected health information covered by an authorization form.

EHN should consider these consumer requests but is not required to accept them. The practice generally accepts a request for a restriction on the uses and disclosures that are described in the notice of privacy practices or outlined in an authorization only if the following criteria are met:

- The request will not impede treatment, payment, or day-to-day functioning of the practice.
- The restrictions will not interfere with the purpose for which an authorization is being sought.
- The consumer has valid reasons for requesting the restrictions, in the judgment of the consumer's mental health professional.

One instance in which the practice will be required to accept the requested restriction is when a consumer has requested a restriction on a release of information to a third-party payer for a service, he or she has already paid for in full out of pocket. In that instance, the provider must accept the individual's request for restriction, unless it is otherwise prohibited by law.

Once EHN accepts requested restrictions, they must be honored unless doing so would interfere with emergency treatment.

All restrictions to which the practice agrees must be documented in writing. Template of the Confidential Communications Form is in Appendix A.

### **Receipt of Request for Confidential Communications**

Written request – A consumer’s request for communications of PHI at an alternative address or by alternative means must be in writing.

- Log in request:
  - Upon receipt of a written request, log in the request in the EHN’s electronic health record.
  - Log in a reminder to respond within ninety (90) days after receipt of the request.
- Identification - Upon receipt of a written request, obtain identification of the requestor.

## 1.34.2 Requestors Who Identify Themselves as Consumer Representatives

### **Procedure**

When the requestor is not the consumer but identifies him or herself as representing the consumer, consider the request in the following circumstances:

- The requestor is an adult consumer’s guardian – Obtain a copy of the court order appointing the requestor as guardian, or a written and notarized statement that a court appointed the requestor as the consumer’s guardian and the appointment still is valid.
- If a guardian has not been appointed and the requestor is the consumer’s agent under a health care power of attorney or mental health care power of attorney – Obtain the signed, valid medical power of attorney naming the requestor as the consumer’s agent and confirm with the consumer’s mental health professional that the consumer is unable to make his or her own health care decisions.
- If a guardian has not been appointed and the consumer does not have a health care or mental health power of attorney, the requestor is directly involved in the consumer’s care or payment for health care. The consumer is present, or is otherwise available prior to the disclosure, and has the capacity to make health care decisions, Emergence Health Network may discuss this information with the family and these other persons if the consumer agrees or, when given the opportunity, does not object. Emergence Health Network may also share relevant information with the family and these other persons if it can infer, based on professional judgement, that the consumer does not object. Confirm the requestor is a person on the following list and a person at a higher level of priority is not immediately available:
  - The spouse, unless the consumer and spouse are legally separated.
  - An adult child.
  - A parent.
  - If the consumer is unmarried but has a domestic partner—if no other person has assumed any financial responsibility for the consumer.

- An adult brother or sister.
- A close friend of the consumer. This must be an adult who has exhibited special care and concern for the consumer. One who is familiar with the consumer's health care news/desires and who is willing and able to become involved in the consumer's health care and to act in the consumer's best interests.

Confirm with the consumer's mental health professional that the consumer is unable to make his or her own decisions.

- The requestor is a minor consumer's parent or guardian.
  - Review the records to determine whether the consumer has been considered emancipated or is otherwise competent to give informed consent. If so, require written consent from the consumer before providing parent or guardian access to records.
  - Before copying or otherwise providing access to records to the requestor, review the records to determine whether the consumer received reproductive health services. If so, contact the Administrative Director of Health Information before granting access to or copying records.
  - Obtain identification verifying the requestor is the parent or guardian.

The requestor is a person entitled to see the records of a deceased consumer if the requestor was involved in the consumer's health care or payment for care prior to the consumer's death, unless doing so is inconsistent with any prior expressed preference of the deceased individual that is known to Emergence Health Network. The information disclosed is limited to that which is relevant to the person's involvement in the consumer's care or payment for care.

### 1.34.3 Time Frames for Responding to Requests for Confidential Communications

#### **Procedure**

EHN will notify the requestor of its decision on a request for confidential communications as soon as practicable and, as a guideline only, should attempt to do so within fifteen (15) days of the request.

Medical Records Associates processing a request for confidential communications will log these dates in the EHN's electronic health record.

### 1.34.4 Determining Whether to Agree to or Deny Request for Confidential Communications

#### **Procedure**

EHN will grant a request for confidential communications so long as the request is reasonable. Associates will take into account the following factors:

- The ability of EHN to comply with the request.
- The resources and time needed to be devoted to compliance with the request.
- Whether the consumer has provided an alternative address or other acceptable alternative means of communication.

- Whether the consumer has made acceptable arrangements for billing.

EHN will not ask the consumer why the consumer is asking for more confidential communications.

All denials for requests for confidential communications should be approved by the Privacy Officer.

A restriction on the disclosure of information that a consumer requests and that the practice agrees to does not prevent the practice from disclosing information that is mandated by law, which does not ever require the consumer's authorization.

- A consumer may request a restriction on the use or disclosure of information at the time he or she signs an acknowledgment of receiving the notice of privacy practices or an authorization form.
- The request should be reviewed by the Administrative Director of Health Information or by an EHN Associate designated by the Administrative Director of Health Information to determine whether the requested restriction would impede the use of information for treatment, payment, or health care operations.
- The Administrative Director of Health Information or the designated EHN Associate should ask the consumer to explain why he or she is seeking the restriction.
- The restriction should be agreed to if, in the judgment of the Administrative Director of Health Information, it will meet the requirements set out in this procedure.
- If the request is agreed to, it should be documented on the authorization form to which it applies.

#### 1.34.5 Termination of Restrictions on Use and Disclosure

EHN may terminate a restriction on the use and disclosure of protected health information to which it has agreed, with the exception of any restrictions it is required by law to accept.

Consumers must be notified of any termination of a restriction and must be given an opportunity to agree or disagree with the termination.

- If the consumer agrees to the termination, information collected before the date of the termination may be used or disclosed as though the restriction had never been accepted.
- If the consumer does not agree to the termination, only information collected after the date of the termination may be used or disclosed without considering the restriction. The restriction will continue to apply to information collected before the date of the termination.

The termination of a restriction must be attached to the authorization form in which the restriction appears.

- An EHN Associate who wishes to terminate a restriction should contact the Administrative Director of Health Information and discuss the need for the termination

- The termination request should be approved if the continuation of the restriction would substantially impede treatment, payment, or the day-to-day operation of the practice.
- Associates should contact the consumer to discuss the need for the termination and to seek the consumer's agreement.
- If the consumer agrees to end the restriction, he or she should sign a statement to that effect. If the consumer is not available to sign a written statement, his or her oral agreement should be noted, signed, and dated by the Associate who discussed the termination with the consumer.
- The termination of the restriction should be attached to the authorization form in which the restriction appears.

### 1.34.6 Consumer Requests for Confidential Communication

EHN Associates must accommodate a consumer's request for confidential communication if the following criteria are met:

- If a consumer desires to have communication from EHN transmitted to a different location other than what is documented in the client file, the EHN Associates shall complete a confidential communications form. Requests for confidential communication must be made in writing. The Associates may provide the consumer with a confidential communication request form.
- The request can be accommodated only without limiting the ability of EHN to submit claims to the consumer's health plan. If the request for confidential communication will prevent the practice from submitting claims to the consumer's health plan, the request will be accommodated only if the consumer identifies another method of paying for services provided by EHN.

The Associates may not require the consumer to explain why he or she wants to receive confidential communications, although the Associates is permitted to request such an explanation. The consumer may refuse to provide any explanation or justification for his or her request.

## 1.35 Facsimile Transmission of Protected Health Information

It is the policy of EHN to protect the privacy and confidentiality of PHI transmitted by facsimile (fax) and hold employees responsible for following the proper procedure when PHI is sent via facsimile to patients and customers. Facsimile transmissions should include the EHN approved fax cover sheet containing a confidentiality statement. The associate must include on the fax cover sheet the name and fax number to whom the fax is going and the name and phone number of the person sending the fax at a minimum.

PHI may be transmitted by facsimile pursuant to EHN privacy policies. Information transmitted must be limited to the minimum necessary to meet the requestor's needs.

### 1.35.1 Outgoing Faxes

### **Procedure**

The fax cover sheet containing a confidentiality statement approved by the Medical Records Supervisor must be used. The cover sheet must also contain directions for the recipient if he/she receives a misdirected fax.

Frequently dialed fax numbers should be programmed into the fax server and checked frequently to assure accuracy.

If the number dialed is not pre-programmed into the fax server, it should be double- checked for accuracy prior to sending the fax.

## 1.35.2 Incoming Faxes

### **Procedure**

Any fax received in error should be reported to the sender and disposed of as directed by the sender.

## 1.35.3 Misdirected Faxes

### **Procedure**

If a fax transmission containing PHI is not received by the intended recipient because of a misdial, check the internal logging system of the fax server to obtain the misdialed number.

If possible, a phone call should be made to the recipient of the misdirected fax requesting the entire content of the misdirected fax be destroyed. If the recipient cannot be reached by phone, a fax should be sent to the recipient requesting the entire fax transmission be destroyed.

Any instance of transmitting PHI to the wrong destination number must be tracked pursuant to Accounting of Disclosures Policy.

## 1.36 Personal Representatives

Emergence Health Network will recognize personal representatives pursuant to applicable privacy regulations. A personal representative may act on behalf of the consumer for the purposes of authorizing use and disclosure of protected health information; or receiving information that otherwise would be sent to the consumer.

### 1.36.1 Designation of a Personal Representative

#### **Procedure**

A personal representative may be the spouse, adult child, or other member of the consumer's family. A personal representative also may be a close friend, or any individual legally authorized to make medical decisions on behalf of the consumer if he or she is incapacitated or otherwise unable to make decisions.

A consumer may designate a personal representative in writing. However, a person who is identified in the consumer record as having legal authority to act on behalf of the consumer will be recognized as a personal representative.

A parent or legal guardian of an unemancipated minor (generally a child under the

age of 18) will be recognized as a personal representative of the child.

- Emergence Health Network’s associates should ask the consumer to identify an individual or individuals who may act as the consumer’s personal representative on the acknowledgment form.
- If a consumer becomes incapacitated, a person accompanying the consumer will be recognized as the consumer’s personal representative if he or she can present evidence of having legal power of attorney or other legally recognized authority to make medical decisions on behalf of the consumer.
- The parent or legal guardian of an unemancipated minor will be recognized as the personal representative of a child, subject to the restrictions contained in **section 1.37**.

### 1.36.2 Authority of Personal Representative

#### **Procedure**

If a consumer is incapacitated, a personal representative may sign any form (such as authorization, revocation of authorization, and request for access to information), the uses of which are described in this privacy manual.

A personal representative may receive protected health information concerning the consumer necessary to carry out the representative’s legal duties to the consumer (for example, providing an informed consent to treatment, or for enforcing an advance directive concerning life support).

### 1.36.3 Refusal to Recognize Personal Representative

#### **Procedure**

An EHN Associate may refuse to disclose information to a person identified as a consumer’s personal representative if the Associate believes that disclosing such information may endanger the consumer.

- An EHN Associate who believes that disclosing information to a personal representative may endanger the consumer should notify their immediate supervisor.
- Requests from the personal representative for information concerning the consumer should be referred to their immediate supervisor.

## 1.37 Parental Access to Protected Health Information Concerning Children

#### **Procedure**

A parent, guardian, or other person recognized by state law as acting in loco parentis on behalf of a consumer who is an unemancipated minor will be recognized as the consumer’s personal representative unless the minor has consented to treatment.

*Note—In this procedure the term “parent” refers to a parent, guardian, or other person acting in loco parentis.*

A parent may act as a personal representative unless state or other law permits

the minor to request that information not be shared with a parent, guardian, or other person acting in loco parentis. Refer to Family Code Chapter 32 in Appendix A.

Generally, EHN requires a parent or legal guardian's signature on any authorization forms for a minor consumer unless the consumer requests that his or her parents not be notified and there is no prohibition under state law in withholding information from the consumer's parent.

- The Administrative Director of Health Information should review any minor's request for confidentiality pertaining to the use or disclosure of protected health information that relates to a parent or guardian to determine whether the request complies with state and federal laws.

## 1.38 Disclosure of Information to Family Members

### **Procedure**

Protected health information concerning a consumer may be disclosed to a family member, other relative, or close friend of the individual who requires the information to assist in the consumer's care and treatment.

- If the consumer can, he or she must agree to the sharing of this information before it occurs. Consumers should generally be asked whether information may be shared with family members. However, permission can be assumed if the consumer has an opportunity to object to disclosure of information to family members and does not do so.
- If the consumer is incapacitated, an EHN Associate may exercise their professional judgment in determining when it is in the consumer's best interests to disclose protected health information to the family member.

The information that may be disclosed to a family member, relative, or close friend is limited to information directly relevant to the family member's involvement in the consumer's care.

- If possible, disclosure of information to others should occur when the consumer is present or after the consumer has agreed to the disclosure.
- If the consumer is present or available for consultation concerning the disclosure, he or she should be given an opportunity to object to the disclosure. If the consumer objects, the information should not be disclosed.
- If the consumer is not present or available for consultation or is incapable of agreeing or objecting to the disclosure, the mental health professional should exercise his or her best professional judgment to determine whether disclosure is in the best interest of the consumer.
- If the consumer agrees to the disclosure or the disclosure is determined to be in the best interest of the consumer, only that information that is directly relevant to the family member's involvement in the consumer's care should be disclosed.

## 1.39 Consumer Access to Protected Health Information

Consumers have the right to receive access to their protected health information

under the HIPAA privacy regulations. It is the procedure of Emergence Health Network to ensure that these rights are met.

### 1.39.1 Consumer Requests for Access to Protected Health Information

#### **Procedure**

A consumer or a consumer's representative may, subject to approval under **section 1.39.3**, inspect and obtain a copy of consumer information maintained in medical records of Emergence Health Network.

- A consumer must submit a request to inspect or copy protected health information as provided for in **section 1.39.2**.
- The request will be reviewed under **section 1.39.3**.
- If the request is denied, the consumer will be informed as provided for in **section 1.39.4**.
- If the request is approved, the consumer will be given access to the requested information as provided under **sections 1.39.5–1.39.8**.

### 1.39.2 Requests for Access to Protected Health Information

#### **Procedure**

A consumer must request in writing an opportunity to inspect or copy his or her protected health information.

This procedure does not address or prevent a mental health professional from sharing the results of laboratory or other diagnostic tests with a consumer or a consumer's personal representative, or from discussing the results of medical procedures. These communications related to treatment may be made orally or in writing at the discretion of the consumer's mental health professional.

This procedure does not address or prevent other Associates from discussing or disclosing to the consumer, orally or in writing, information related to the current status of claims that have been submitted to the consumer's health plan.

- When a consumer or the consumer's representative 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 consumer should be referred to the Medical Records Supervisor.
- The Medical Records Supervisor will give the consumer or the consumer's representative a copy of a request form and explain EHN's policies on allowing consumers to inspect their information.
- Upon receipt of a request form, the Medical Records Supervisor will review the request as explained in **section 1.39.3**.

### 1.39.3 Review of Consumer Requests for Access to Protected Health Information

#### **Procedure**

The request for access to personal health information will be sent promptly to the Medical Records Supervisor. A copy of the request will be filed in the consumer's records.

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

A decision to grant the consumer or the consumer's personal representative permission to inspect or copy the requested information will be made within 30 days of the date the request is submitted.

If the protected health information is maintained in electronic form and the consumer would like to view the information or receive a copy of it in electronic form, he or she must make that request specifically on the request form.

### **Restrictions on Access**

- Information compiled in anticipation of, or for use in, legal proceedings will not be made available to the consumer or the consumer's legal representative unless required by law or court order.
- Information that, by law, may not be disclosed to the consumer will not be made available to the consumer or the consumer's representative.
- Information will not be made available if the consumer's mental health professional believes that it is likely to endanger the life or physical safety of the consumer.
- Information will not be made available if the consumer's mental health professional believes that access to the information is reasonably likely to cause substantial harm to a person other than the consumer who is referenced in the consumer's records.
- Information will not be made available to a personal representative of the consumer if the consumer's mental health professional believes that access to the information by the personal representative is reasonably likely to cause harm to the consumer or to another person.

The Medical Records Supervisor will review the request to inspect or copy protected health information and will contact the consumer's mental health professional to determine if there are any reasons to restrict the consumer's or consumer representative's access to the information.

If the request is disapproved, wholly or in part, the consumer will be notified using the procedures outlined in **section 1.39.4**.

If the request is approved, the consumer will be notified, and arrangements made for the consumer to inspect or copy the requested information using the procedures described in **sections 1.39.5– 1.39.8**.

## **1.39.4 Communication of Denial of Requests for Access to Personal Health Information and Review of Decision to Deny Access**

### **Procedure**

A written explanation of the denial of a consumer's request to inspect or copy protected health information will be prepared using the appropriate form. If an alternative, such as a summary of the requested information, could satisfy the consumer's request at least in part, the communication should describe that

alternative.

A consumer or the consumer'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.

- When the Medical Records Supervisor receives a copy of the denial notice indicating that the consumer is requesting a review of the denial, the privacy official should forward the request to a licensed health professional who was not involved in the original denial and ask the mental health professional to review the decision.
- The review should normally be completed within 30 days. The Medical Records Supervisor will follow up with the reviewing mental health professional if the review is not completed within 30 days.
- The Medical Records Supervisor should communicate the result of the review to the consumer using the reviewer form.

### 1.39.5 Inspection of Records

#### **Procedure**

Upon request by consumer or their authorized personal representative records shall be made available to the consumer within 15 business days from the date the request is made for records available through the consumer's electronic health record or within 30 calendar days if the record is in hard copy format. This time frame may be extended pursuant to state or federal regulations.

### 1.39.6 Communication of Decision to Permit Inspection or Copying of Protected Health Information

#### **Procedure**

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

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

- The Medical Records Supervisor will determine the earliest date at which the requested information can be made available.
- The Medical Records Supervisor or a designated associate will prepare the approval form and send it to the consumer.

### 1.39.7 Arrangements for Inspection of Protected Health Information by Consumers

#### **Procedure**

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

The consumer must inspect the records on the premises of EHN. If this is not satisfactory to the consumer, he or she should be given the option of having copies made and sent to an address that he or she specifies. However, the consumer may be charged the cost of preparing and mailing the copies or for the

supplies and labor to put together the electronic version for mailing.

### 1.39.8 Fees for Copying Personal Health Information

#### **Procedure**

If the consumer or personal representative requests copies of personal health information maintained by EHN, he or she will be charged a flat fee of **\$6.50**. Flat fee rate applies when consumer requests to have the copy sent to him/her, or as directed by the consumer to send the copy to a third party (it doesn't matter who the third party is). The consumer must submit this request in writing and signed by the consumer when sending to a third party. When request for copies from a third party are forwarded to Emergence Health Network at the direction of the consumer the flat rate fee will apply.

If the consumer requests their records be put onto a disk or USB drive, he or she will be charged a flat fee of **\$6.50**.

If it is deemed that the person is indigent and does not have this fee, it can be waived. Emergence Health Network will not charge for the first set of copies made or for the establishment of a disability claim.

If a third party directly requests the consumer records the flat fee rate of **\$6.50** will apply to the third party (attorneys). If it is unclear whether the request was from the consumer or from the third party the associate may clarify with the consumer.

## 1.40 Amendment of Health Information

Consumers have the right to request that amendments be made to their protected health information under the HIPAA privacy regulations. It is the procedure of Emergence Health Network to ensure that these rights are met.

#### **Procedure**

A consumer may request amendment of the information maintained by Emergence Health Network in the designated record sets listed below. The consumer must follow the procedures outlined in **section 1.40.1** when requesting amendment of information maintained by Emergence Health Network.

#### **Designated Record Sets**

Consumers may request amendments to information contained only in the following record sets:

- The consumer's medical records
- The consumer's billing records
- Other records that contain protected health information used to direct treatment

### 1.40.1 Procedures for Requesting Amendment of Information

#### **Procedure**

Requests to amend protected health information must be submitted in writing. Consumers should use the consumer information amendment form.

- Consumers who indicate their belief that the information in their records is

incorrect should be given a consumer information amendment form.

- Consumers should be referred to the Medical Records Supervisor to resolve questions about the form.

## 1.40.2 Action on Requests for Amendment of Information

### Procedure

The Medical Records Supervisor may deny a consumer's request to amend records if the following criteria are met:

- The information to be amended was not created by Emergence Health Network but was received from another entity.
- The information to be amended is accurate and complete- i.e. there is no need for the information to be amended.
- The information to be amended does not exist in the specified records.
- The information to be amended is not available for inspection by the consumer or the consumer's representative (see **section 1.39.1**).

Action must be completed on any request for amendment within 60 days of receiving the request. If action cannot be completed within 60 days, EHN must notify the consumer of the delay, including the reasons for the delay, and complete the review within 90 days of the date the request was originally received.

- Consumer information amendment forms should be forwarded to the Medical Records Supervisor.
- The Medical Records Supervisor should contact the consumer's mental health professional or Associates (clinic supervisors) he or she designates and request a review of the requested amendments.
- The mental health professional or designated Associates should indicate which of the requested amendments should not be made because the information in the consumer's record is accurate and complete or meets the other requirements for denying a request that are listed above
- The mental health professional or designated Associates should then return the form to the Medical Records Supervisor.
- The Medical Records Supervisor should review the form after it is returned by the consumer's mental health professional and identify any information that should be amended.
- The Medical Records Supervisor should initiate the procedures for amending protected health information specified by **sections 1.40.4 – 1.40.5**.
- The Medical Records Supervisor should prepare a response to the consumer as required by policies in **sections 1.40.6–1.40.8**.

## 1.40.3 Communication of Decision on Requests for Amendment of Information

### Procedure

After completing the review of a consumer's request for amendment of protected health information, the Medical Records Supervisor will complete the consumer information amendment form by indicating the disposition of each requested

amendment.

A copy of the completed consumer information amendment form will be sent to the consumer along with any explanatory comments that the Medical Records Supervisor believes to be necessary.

The consumer will be asked to submit the names and addresses of any organizations or individuals that he or she has reason to believe have received the uncorrected information for the purpose of notifying them of the amendment.

#### 1.40.4 Procedures for Amendment of Internal Records

##### **Procedure**

When a consumer's request for amendment of protected health information is approved, either of the following procedures should be followed:

- The records containing the affected information are updated.
- The amended information is linked to the original information.

The Medical Records Supervisor will refer the request for amendment to EHN Associates responsible for maintaining the affected records and will identify the records that need to be amended. Those records should either be amended or be linked to the amended information (that is, contained in a new or corrected record where it will be available when the affected information is used or disclosed in the future).

#### 1.40.5 Notifying Other Parties That Information Has Been Amended

##### **Procedure**

When a consumer's protected health information is amended in response to a consumer's request, other organizations to which the information being amended has been disclosed will be notified of the amendment.

Organizations to be notified include:

- Business associates, health plans, and other providers the Medical Records Supervisor can identify as having received the information
- Persons and organizations the consumer can identify as having received the information that requires amendment, but only to the extent that the Medical Records Supervisor can confirm that these persons or organizations previously received the information

EHN is not required to confirm that the organizations or other entities notified of the amendment have updated their records.

#### 1.40.6 Denial of Request for Amendment

##### **Procedure**

When a request to amend protected health information is denied, the consumer will be informed of the decision in writing. The notice sent to the consumer must advise the consumer of the following:

- The consumer may submit a statement of disagreement that will become part

of his or her records and will, in the future, be disclosed to any person or organization that receives the identified information.

- If the consumer does not submit a statement of disagreement, he or she may ask EHN to include the request for amendment and the denial in any future disclosure of the identified information to any person or organization that receives the identified information.
- The consumer may file a complaint with the provider concerning the request for amendment  
(a description of how the consumer can file this complaint must be included in the notice).

The letter must identify the name, mailing address, and telephone number of the Administrative Director of Health Information.

#### 1.40.7 Statement of Disagreement

##### **Procedure**

If the consumer disagrees in writing when notified that a request for amendment of protected information has been denied, the Medical Records Supervisor will review the objection and append or link it to the consumer's record. This will ensure that the objection will accompany the original information when it is used or disclosed in the future.

The Medical Records Supervisor may prepare an accurate summary of the consumer's statement of disagreement if he or she believes that a summary will adequately provide a clear understanding of the disputed information.

#### 1.40.8 Rebuttal of Disagreement

##### **Procedure**

If a consumer disagrees in writing when notified that a request for amendment of protected health information has been denied, the Administrative Director of Health Information will review the statement and determine whether a formal rebuttal or response, as provided for in federal regulations, is necessary. If it is determined that a rebuttal is necessary, the privacy official will prepare and append it to the consumer's records.

- The Administrative Director of Health Information will consult as necessary with the consumer's mental health professional or other EHN Associates to make this determination.
- Both the consumer's statement of disagreement and the rebuttal statement will be noted in the consumer's records.
- The statement of disagreement and the rebuttal will be either included in the consumer's records or linked to those records to permit them to be included with the original information when it is used or disclosed in the future.
- A copy of the rebuttal statement will be sent to the consumer.

#### 1.40.9 Receipt of Notification of Amendment

##### **Procedure**

When notified by another medical practice, health plan, or other covered entity that protected health information received earlier has been amended, EHN will follow

the procedures in place for handling its own amended information.

## 1.41 Accounting to Consumers for Disclosures of Information

Consumers have the right to request an accounting of specific types of uses and disclosures of their protected health information made under the HIPAA privacy regulations.

### 1.41.1 Procedure to Request an Accounting of Disclosures

#### **Procedure**

To receive an accounting of disclosures of protected health information, a consumer must submit a written request to the Medical Records Supervisor.

- A consumer who indicates to any EHN Associates that he or she would like to receive an accounting of disclosures should be informed to contact the Medical Records Department.
- The Medical Records Department will provide the consumer with a disclosure accounting form and review the types of disclosures that will be reported in the accounting.
- The Medical Records Supervisor will determine whether the ability of the consumer to obtain an accounting of disclosures has been suspended in response to a request from a law enforcement or health oversight agency.
- If the consumer's right to an accounting has not been suspended, the Medical Records Department will start preparing an accounting.

### 1.41.2 Charges for Accountings of Disclosures

#### **Procedure**

If a consumer requests more than one accounting during any 12-month period:

- The consumer will not be charged for the first accounting.
- If the consumer received an accounting for which he or she was not charged during the preceding 12 months, he or she will be informed that EHN will charge \$ 6.50 for the second accounting. If the consumer agrees to pay this fee, the accounting will be provided.

### 1.41.3 Suspension of a Consumer's Right to Receive an Accounting of Disclosures

#### **Procedure**

A law enforcement or health oversight agency may request the provider to suspend the right of an individual to request an accounting of disclosures. Requests from law enforcement agencies should be submitted in writing. The written statement should indicate that providing an accounting is likely to impede the agency's activities and should specify a time period during which the consumer's right will be suspended.

Suspensions that last more than 30 days must be supported in writing, and requests must be made in writing. If a written request is not submitted, the individual's right to an accounting may be suspended for no more than 30 days.

- A communication from a law enforcement or health oversight agency requesting the suspension of a consumer's right to an accounting of disclosures should be directed to the Administrative Director of Health Information.
- The Administrative Director of Health Information will verify the credentials of the government official that makes a verbal request and document the identity of the official or agency.
- The Administrative Director of Health Information will place the consumer's name on a list of persons whose right to an accounting has been suspended pursuant to an official request.

#### 1.41.4 Information to Be Provided in an Accounting of Disclosures

##### **Procedure**

The information that will be provided in an accounting of disclosures includes:

- The date of the disclosure
- The name of the entity or person who received the protected health information
- A brief description of the purpose of the disclosure or a copy of the authorization for the disclosure

*Note: Disclosures to business associates for purposes of treatment, payment, and health care operations should not be included in the accounting.*

#### 1.41.5 Documentation of Accountings Provided to Consumers

##### **Procedure**

Copies should be made of all accountings of disclosed information prepared for consumers. The copies should be kept for six years.

#### 1.41.6 Documentation of Disclosures Requiring an Accounting

##### **Procedure**

When an Associate discloses protected health information, the Associate will document the disclosure. This documentation would be necessary if the consumer were later to request an accounting of disclosures.

- Any disclosure, other than a disclosure for purposes of treatment, payment, or health care operations, will be documented by completing a disclosure accounting form.
- The disclosure accounting form will be forwarded to the Medical Records Clerk, who will update the files and databases that are used to prepare accountings of disclosures.

### 1.42 Submission of Complaints

A process has been adopted by Emergence Health Network by which complaints regarding potential privacy violations can be submitted for investigation to the Administrative Director of Health Information.

##### **Procedure**

Associates shall report complaints via Ethics Point Incident Management (or a successor ethics hotline implemented by EHN). A consumer or other individual who wants to file a complaint concerning EHN's privacy policies and procedures, or a suspected disclosure of protected health information that violates federal or state law should:

- Be directed to the Administrative Director of Health Information for answers to questions about filing complaints
- Receive a copy of the complaint form from the Administrative Director of Health Information to be returned by mail to the address printed on the form.

## 1.43 Complaint Resolution Procedures

Emergence Health Network will work to resolve every complaint raised by an individual. All potential violations of privacy will be investigated.

### 1.43.1 Complaints Concerning Privacy Policies and Procedures

#### **Procedure**

The procedures for resolving complaints submitted by consumers or other individuals concerning the privacy practices of Emergence Health Network or the policies and practices established in this manual are outlined below.

- Upon receiving a complaint, the Administrative Director of Health Information or a designated Associates will review the complaint, evaluate the specific details of the complaint, and determine whether the complaint warrants a change in the privacy policies or procedures of EHN.
- If a change appears to be warranted, the Associates conducting the evaluation will develop a recommendation and submit it to the Administrative Director of Health Information, who will determine whether an immediate change in policies and procedures is needed to prevent a violation of federal or state privacy standards, laws, or regulations.
- If it is determined that a change in policies and procedures is necessary; a revised procedure will be prepared following the procedures outlined in **section 1.8**. The Administrative Director of Health Information should prepare a response and send it to the individual submitting the complaint. The response should thank the individual for his or her interest. It should indicate that the suggestion has been evaluated, and that EHN believes that its current procedures comply with federal and state requirements
- If a change does not appear to be warranted, the Administrative Director of Health Information will prepare a response and send it to the individual submitting the complaint. The response should thank the individual for his or her interest and indicate that the suggestion has been evaluated but that EHN believes that its current privacy procedures comply with federal and state requirements and are sufficient to protect consumer privacy.
- Receipt of the complaint and its final disposition should be documented using the procedures outlined in **section 1.43**.

### 1.43.2 Complaints Arising from Possible Violations of Privacy Policies

## Procedure

The procedures for resolving complaints submitted by consumers or other individuals concerning the disclosure of protected health information are outlined below.

- An Associate who receives a complaint from a consumer or other individual that concerns a possible use or disclosure of protected health information that violates EHN's privacy policies and procedures, or that violates federal and state law, should immediately refer the complaint to the Administrative Director of Health Information.
- The Administrative Director of Health Information will review the complaint and determine whether a violation occurred and, if so, whether the violation involves only the privacy policies and procedures established in this manual or also involves a violation of federal and state privacy laws and standards.
- If the Administrative Director of Health Information determines the complaint may involve a violation of federal or state standards and legal requirements, he or she will immediately forward the complaint to EHN's legal counsel for evaluation. The request for evaluation should specify a date by which the evaluation should be completed.
- The Administrative Director of Health Information should follow up and track the status of the referral. If the evaluation indicates that federal or state standards may have been violated, the mitigation procedures established in **section 1.44** should be followed.
- If the Administrative Director of Health Information determines that the complaint does not involve a violation of federal or state standards and legal requirements, he or she will determine whether EHN's privacy policies and procedures were violated. If policies and procedures have been violated, the disciplinary procedures established by **section 1.6** should be initiated.
- The Administrative Director of Health Information should contact the person submitting the complaint and notify him or her of the actions that will be taken to address the complaint.
- Evaluations of complaints should generally be completed within 30 days of receipt.
- The receipt of the complaint and the final disposition should be documented using the procedures established in **section 1.43**.

### 1.43.3 Documentation of Complaints

#### Procedure

The Administrative Director of Health Information will establish and maintain files containing documentation of all complaints received. This documentation will include the actions taken to address or resolve the complaint, including any written correspondence with the person submitting the complaint. Documentation will be completed within Ethics Point Incident Management or a successor HIPAA compliance program implemented by EHN.

## 1.44 Mitigation

Emergence Health Network will mitigate to the extent possible any harmful effects

resulting from the use or disclosure of protected health information that violates Emergence Health Network policies and procedures, or the requirements of state and federal law.

### **Procedure**

When Administrative Director of Health Information determines that a use or disclosure of protected health information has violated the policies and procedures established by this manual, the case will be referred to EHN's legal counsel to:

- Determine any action needed to mitigate any harm that may result to the consumer whose information was used or disclosed
- Evaluate EHN's legal exposure and recommend a course of action
- Follow up with the consumer

All communications with the consumer concerning use or disclosure of protected health information that legal counsel determines may violate federal or state standards and legal requirements should be handled by EHN's legal counsel.

## **1.45 Non-retaliation and Protection for Whistleblowers**

Emergence Health Network will ensure that no retaliatory action will be taken against consumers, associates, or any others that bring to the organization's attention a potential privacy violation.

### **Procedure**

As an organization, EHN does not partake in any type of intimidation, threats, coercion, discrimination, or other retaliatory action against any persons that bring to the attention of the organization or the HHS OCR potential issues in privacy practices. Any issues brought directly to the Administrative Director of Health Information will be investigated, and appropriate sanctions will be applied in the event that an issue is found.

---

# Section 2—Breach Incident Management Policies and Procedures

This section addressing breach incident management policies and procedures is divided into three parts. It addresses prevention of breaches, investigating potential breaches, and communication about breaches to consumers and others. Each part contains policies, procedures, and forms designed to help providers take immediate action when needed.

## Preventing Breaches

### 2.1 Mobile Device Inventory

The loss or theft of mobile devices is most often associated with unauthorized disclosure of protected health information. In many instances, the missing device is not discovered immediately. This procedure ensures more timely discovery and recovery. Most discoveries of breaches are through audit and assessment.

In an effort to prevent unauthorized disclosure of consumers' protected health information, Emergence Health Network will conduct an annual inventory of all mobile devices for clinical and administrative operations. This inventory includes all devices involved in the creation, storage, and transmission of electronic protected health information within Emergence Health Network. The Administrative Director of Information Technology will conduct the inventory.

Devices that are lost or otherwise cannot be addressed in this inventory will be considered at risk for breach of electronic protected health information and investigated by Administrative Director of Health Information immediately. A device that cannot be located within 24 hours following the inventory, or is noted to be missing at any time, will be regarded as lost or stolen and its content to have been breached unless the use of encryption has been installed.

#### **Procedure**

This inventory will be conducted annually or more frequently at any time the Administrative Director of Information Technology believes this action is warranted. Before an electronic device is assigned to an employee, it will be given a unique identification number that will be written on or attached to a tag (e.g. asset tag) on the device. These numbers will be kept on a list. When a device is assigned to an employee, the employee's name will be recorded along with the device ID number. To confirm possession, the Administrative Director of Information Technology will record the unique identification number assigned to each device and found on the asset tag for each device. In this way, users of the device can confirm to the Administrative Director of Information Technology that the device is in his/her possession.

#### **Electronic Device Inventory Form**

List all types of devices, tag number and who owns or has access. All devices are considered to carry protected health information.

### 2.2 Mobile Device Protection

According to the Office for Civil Rights breach report, theft and loss of mobile devices is a primary source of breaches. Employee negligence is the cause.

Emergence Health Network recognizes that theft and loss of mobile devices is a primary source of unauthorized disclosures of consumers' protected health information. This procedure includes commonsense steps to secure laptop computers and other portable electronic devices, such as tablets.

While the replacement cost of devices is significant, loss of data containing consumers' protected health information or confidential company information is far more serious.

### **Procedure**

**Automobiles**—Very often laptops are stolen from unlocked, and locked, automobiles. For this reason, laptops and other devices must be transported in the trunk or otherwise placed out of sight in vehicles without trunks. (Laptops should not be left in an automobile unattended, unless unavoidable.)

**Home**—Thefts from home can occur during break-ins and when homes are visited by maintenance, delivery, or repair personnel. Keep devices secured.

**Travel**—Do not leave laptops or other devices unsecured in hotel rooms. Keep your laptop with you or place it in the hotel room safe or use a security cable.

**Protective Measures** -Aside from theft, simple negligence often results in the loss of devices. Stay attached to your laptop with a strap that stays over your shoulder at all times.

Passwords and IDs associated with your laptop and the systems that it can access must never be stored with or on the computer.

When a mental health professional or employee is issued an electronic device, he or she must review the above rules and Emergence Health Networks Mobile Device Procedure; a signature will be required as acknowledgment of their understanding.

### **Mobile Device Inventory Form**

This form lists employees who have been issued a mobile device, device number, and notes whether they have received and read the Mobile Device Procedure.

## **2.3 Confidential Information**

Some analyses of unauthorized disclosures note that employees often use consumer data inappropriately. The purpose of this procedure is to make clear to employees the limits of their access to consumer information and to remind them that impermissible use is subject to sanctions, including civil and criminal fines and penalties.

Emergence Health Network will be aware of and agree to the limitations on access to consumer and company information. New employees will receive a copy of this procedure at their orientation, and all employees will receive this information annually. Employees will be required to acknowledge by their signature that they have received this notice regarding consumer confidential information.

Further, employees are advised that their access to consumer information and other company information may be monitored and that access to documents is recorded as part of our security program. At the direction of Administrative Director of Health Information, an audit of employee access of consumer and company information will be conducted.

### **Confidential Information Policy Acknowledgment**

**Confidential Information**—Consumer information is confidential and protected by federal law. Whether intentional or accidental, breach of confidentiality can harm consumers and Emergence Health Network. Federal law provides for penalties—both imprisonment and fines—and may also result in termination of employment, according to employee rules for this organization.

Information relating to consumers, employees, or the business operations of Emergence Health Network— Such information is subject in accordance with HIPAA Regulations, 42 CFR Part2, and following restrictions.

1. Information may be accessed and used only for work-related purposes.
2. Information may not be removed from the organization without permission of the Administrative Director of Health Information.
3. Information may not be shared with persons outside of this organization, unless otherwise authorized by your supervisor.

**Need to know**—All access to confidential information is governed by the need to know and “minimum necessary” standard to perform tasks. Associates may not make any personal use of consumer information or EHN confidential business information.

**Personal and family**—Associates must request permission from the Administrative Director of Health Information to access personal or family member information, which may be subject to limitations requested by family members.

**Report violations**—Associates are required to report any suspected violation of confidential consumer or business information policy to the supervisor or the Administrative Director of Health Information.

## 2.4 Risk Analysis

As mentioned in the HIPAA security rule, covered entities must evaluate the likelihood and impact of potential risks to the confidentiality of electronic PHI maintained in and transmitted using portable devices.

Emergence Health Network will evaluate the likelihood and impact of potential risks at least annually or whenever events require, such as a change in the physical location of the organization or the occurrence of a security breach.

### **Procedure**

The procedure for conducting a risk analysis is contained in Appendix B: Privacy Breach Assessment.

## 2.5 Discovery of a Breach

HIPAA rules note that a breach is considered to have occurred on the day it is known or should have been known. Further, rules require that covered entities and their business associates determine the probability that data have been breached or disclosed to unauthorized individuals, and not the extent to which consumers have been harmed by the disclosure.

As soon as a breach of unsecured protected health information is discovered, it is the procedure of Emergence Health Network to take action. That action may vary based on the situation, but it will not be delayed for any reason.

The circumstances of any breach are noted, and records are kept for seven years.

### **Procedure**

The Administrative Director of Health Information will take action upon discovery of a breach. The action taken may involve investigating, conducting a risk assessment and, if appropriate, beginning notification procedures following the risk assessment.

Under the HIPAA breach notification regulations, a breach of PHI is to be treated as having been “discovered” on the first day the incident is made known to the organization or, by exercising a reasonable amount of diligence, would have been known to the organization. This also includes breaches the organization’s business associates discover.

### **Discovery of Breach Documentation**

Using Ethics Point Incident Management (or its successor), the Administrative Director of Health Information records all information relevant to the discovery of the breach. Note that this information, along with other facts, is used to support the decision to notify or not notify individuals whose PHI is involved. The steps for reporting a possible breach are included as Appendix B

## **2.6 Risk Assessment**

These criteria are noted in the regulations and officially determine whether an actual breach has occurred. (Note a risk assessment is different from a risk analysis, which focuses more broadly on identifying potential threats to privacy and security within this organization.)

An inappropriate acquisition, use, disclosure, or access of information not likely to compromise protected health information is not actually considered a breach. To determine if an actual breach has occurred, a risk assessment must be performed.

### **Procedure**

When a potential breach has occurred, a risk assessment is performed to determine if the protected information has been compromised. The following questions must be answered during this risk assessment:

- What was the extent and nature of the information involved in the case?
- Who is the unauthorized person who received access to the information or to whom was the disclosure made?
- Was the PHI actually acquired or viewed by the unauthorized person?

- To what extent has the risk to the PHI been mitigated?

If there is a low probability of compromise, there is no breach. This must be documented in the investigation records. If a compromise is likely, the investigation continues at that point.

*Investigating and Evaluating the Risks Associated with the Breach*

1. To determine what other steps are immediately necessary, the Privacy Officer in collaboration with the CIO, CCO, CEO and/or EHN’s Legal Counsel if necessary and affected department(s) and administration, will investigate the circumstances of the breach.
2. Associates involved in the discovery or breach must cooperate with Emergence Health Network designated investigating Associates: Privacy Officer, Supervisors, Legal Counsel, Chief Compliance Officer, Chief Information Officer, and other designated associates.
3. Associates involved in the discovery or breach must cooperate with Health & Human Services, Department of State Health Services, Department of Aging and Disability Services, Department of Assistive and Rehabilitative Services, Medicaid Programs, Office of Civil Rights, Office of Inspector General and any other agency during investigations regarding privacy violations and breaches.
  - a. A review of the results of the investigation to determine root cause(es), evaluate risks, and develop a resolution plan.
    - i. The Privacy Breach Assessment tool will help aid the investigation.
  - b. The Privacy Officer, in collaboration with the CIO, CCO, CEO/EHN’s Legal Counsel, will consider several factors in determining whether to notify individuals affected by the breach including, but not limited to:
    - i. Contractual obligations
    - ii. Legal obligations – EHN’s Legal Counsel should complete a separate legal assessment of the potential breach and provide the results of the assessment to the Privacy Officer and the rest of the breach response team
    - iii. Risk of identity theft or fraud because of the type of information lost such as social security number, banking information, identification numbers
    - iv. Risk of physical harm if the loss puts an individual at risk of stalking or harassment
    - v. Risk of hurt, humiliation, or damage to reputation when the information includes medical or disciplinary records
    - vi. Number of individuals affected

**Breach Identification Form**

The form below can be used to identify breaches. It lists the 18 data elements that, whether alone or in any combination, are considered to be protected health information and whose disclosure to unauthorized persons is considered to be a breach, according to the *Code of Federal Regulations*, section 164.514.

Protected Health Information Data Elements	Elements Involved in Breach
1) Names	

<p>2) Five-digit ZIP codes</p> <p>(a) The first three digits of a ZIP code (only the first three) may be used if more than 20,000 people have a ZIP code with the same first three digits; and</p> <p>(b) The first three digits of a ZIP code must be changed to 000 if fewer than 20,000 people have a ZIP code with the same first three digits.</p>	
<p>3) Birth date, admission date, discharge date, date of death; and all ages over 89 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</p>	
<p>4) Telephone numbers</p>	
<p>5) Fax numbers</p>	
<p>6) Electronic mail addresses</p>	
<p>7) Social Security numbers</p>	
<p>8) Medical record numbers</p>	
<p>9) Health plan beneficiary numbers</p>	
<p>10) Account numbers</p>	
<p>11) Certificate/license numbers</p>	
<p>12) Vehicle identifiers and serial numbers, including license plate numbers</p>	
<p>13) Device identifiers and serial numbers</p>	
<p>14) Web Universal Resource Locators (URLs)</p>	
<p>15) Internet Protocol (IP) address numbers</p>	
<p>16) Biometric identifiers, including finger and voice prints</p>	
<p>17) Full face photographic images and any comparable images</p>	
<p>18) Any other unique identifying number, characteristic, or Code</p>	

## 2.7 Breach Incident Investigation

Recent HIPAA rule changes now require that an investigation address the probability that PHI was compromised, not the level of harm potentially incurred by consumers.

This organization will investigate any and all potential breaches of unsecured protected health information.

### **Procedure**

The organization will name the Administrative Director of Health Information to act as the investigator of the breach unless there is a conflict of interest in the situation. This person is responsible for the entire process, from the initial investigation through the notification of individuals and appropriate entities.

### *Containing the Breach*

1. The Privacy Officer will take the following steps to limit the scope and effect of the breach.
  - a. Work with department(s) to immediately contain the breach. Examples include, but are not limited to:
    - i. Stopping the unauthorized EHN
    - ii. Recovering the records, if possible
    - iii. Shutting down the system that was breached
    - iv. Mitigating the breach, if possible
    - v. Correcting weaknesses in EHN's security
    - vi. Notifying the appropriate authorities including the local police department if the breach involves, or may involve, any criminal activity
    - vii. Procedures as required by the Data Use Agreement

### *Prevention*

1. Once immediate steps are taken to mitigate the risks associated with the breach, the Privacy Officer will investigate the cause of the breach.
  - a. If necessary, this will include a security audit of physical, organizational, and technological measures.
  - b. This may also include a review of any mitigating steps taken.
2. The Privacy Officer will assist the responsible department to put into effect adequate safeguards against further breaches.
3. Procedures will be reviewed and updated to reflect the lessons learned from the investigation and regularly thereafter.
4. The resulting plan will also include audit recommendations, if appropriate.

## 2.8 Breach Reporting by Business Associate

Industry literature notes that business associates are often involved in the disclosure of protected health information to unauthorized persons. The purpose of this procedure is to prevent breaches involving business associates and their employees by reminding them of their responsibility to protect consumer information and to take appropriate action when circumstances require.

A business associate must take responsibility and participate fully in breach investigations. This procedure will be provided to all business associates at the start of their contract, and annually thereafter.

A business associate working with Emergence Health Network will follow these procedures and those under the Business Associate Agreement entered into between EHN and business associate. Any conflicts between these procedures and the Business Associate Agreement shall be resolved in favor of the Business Associate Agreement. Attached in Appendix A is a template Business Associate Agreement.

(a)(1) A business associate shall, following the discovery of a breach of unsecured protected health information, notify Emergence Health Network, the covered entity, of such breach.

(2) *Breaches treated as discovered.* A breach shall be treated as discovered by a business associate as of the first day on which such breach is known to

the business associate or, by exercising reasonable diligence, would have been known to the business associate.

A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the federal common law of agency).

(b) *Timeliness of notification.* Except as required by law enforcement, the business associate shall provide the notification required without unreasonable delay and in no case later than 48 hours after discovery of a breach.

(c) *Content of notification.*

(1) The notification shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach.

(2) A business associate shall provide the covered entity with any other available information that the covered entity is required to include in notification to the individual under §164.404(c) at the time of the notification or promptly thereafter as information becomes available. This information includes a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known, and a description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved).

### **Procedure**

The list of 18 protected health information data elements above will be provided to business associates.

## **2.9 Breach Notification to Individuals**

45 CFR section 164.404 lays out the requirements for notifying individuals about disclosures of protected health information to unauthorized individuals.

If it is determined that a breach has occurred, this organization's procedure is to notify the individuals involved in the breach, as well as the Department of Health and Human Services in the appropriate manner based on the breach, and the media if appropriate based on the situation. This notification will be made in a timely manner, in no case later than 60 days following the discovery of the breach, unless there is a delay due to law enforcement purposes.

### **Procedure**

Notice will be provided via first class mail to the individual at his or her last known address, or via email if he or she has previously agreed to receive electronic communication from the organization. If the consumer has refused to receive both mail and electronic communications from the provider, the organization must call the consumer and request that he or she pick up the written notice.

If it is clear that the notice has not reached the individual or if there is no contact information available, a substitute notice may be used.

If there are fewer than 10 individuals for whom there is incorrect or insufficient contact information, a substitute notice must be provided via telephone, an alternative written notice, or other appropriate means.

If there are 10 or more individuals for whom there is incorrect or insufficient contact information, a substitute notice may be in the form of a posting on the main page of EHN's website for ninety (90) calendar days, or the notice may be printed in the local newspaper or disseminated via broadcast media. Notices made to prominent media outlets shall contain the same elements of information as required for the notice to the patient. The notice must include a toll-free phone number which remains active for 90 days that potential involved consumers can call to find out if they were involved in the breach. Notice to prominent media outlets must be completed without unreasonable delay and no later than 60 days after the discovery of the breach.

***Sample Breach Notification Letter is found in Appendix B in the back of this manual.***

*Notification*

1. The Privacy Officer will work with the department(s) involved, EHN's Legal Counsel and appropriate leadership to decide the best approach for notification and to determine what may be required by law.
2. If required by law, notification of individuals affected by the breach will occur pursuant to the Data Use Agreement between the Texas Health and Humans Services Enterprise and EHN and more specifically, to those requirements set under 45 CFR sections 164.400-414 as soon as possible following the breach.
  - a. Affected individuals must be notified without reasonable delay, but in no case later than sixty (60) calendar days after discovery, unless instructed otherwise by law enforcement or other applicable state or local laws.
    - i. Notices must be in plain language and include basic information, including:
      1. What happened- dates of the breach and breach discovery
      2. Types of PHI involved- Full Name, Social Security Number, Date of Birth, Home Address, Account Number, Diagnosis, Disability Code, or other types of information involved
      3. Steps individuals should take to protect themselves from potential harm
      4. Steps covered entity is taking- to investigate the breach, to mitigate the harm to the individual, and to protect against further breaches
      5. Contact Information- that individuals can use to gain knowledge of breach such as toll-free number, email address, website or postal address.

- ii. Notices should be sent by first-class mail or if individual agrees electronic mail. If insufficient or out-of-date contact information is available, then a substitute notice is required as specified below.
  - b. If law enforcement authorities have been contacted, those authorities will assist in determining whether notification may be delayed in order not to impede a criminal investigation.
3. The required elements of notification vary depending on the type of breach and which law is implicated. As a result, EHN's Privacy Officer and Legal Counsel should work closely to draft any notification that is distributed.
4. Indirect notification such as website information, posted notices, media will generally occur only where direct notification could cause further harm, or contact information is lacking.
  - a. If a breach affects five-hundred (500) or more individuals, or contact information is insufficient, EHN will notify the media as appropriate for the size of the location with affected individuals, and notice will be provided in the form of a press release.
5. Using multiple methods of notification in certain cases may be the most effective approach.

Business associates must notify EHN if they incur or discover a breach of unsecured PHI.

1. Notice to EHN must be provided without reasonable delay and in no case later than forty-eight (48) hours after discovery of the breach.
2. Business associates must cooperate with EHN in investigating and mitigating the breach.

Notice to Health and Human Services (HHS), Texas Health and Human Services Commission and all other affected divisions (DADS, DSHS, etc.), as required by HIPAA – If EHN's Legal Counsel determines that HIPAA notification is not required; this notice is also not required.

1. Information regarding breaches involving five-hundred (500) or more individuals, regardless of location, must be submitted to DSHS at the same time that notices to individuals are issued.
2. If a breach involves fewer than five-hundred (500) individuals, EHN will be required to keep track of all breaches and to notify DSHS within sixty (60) days after the end of the calendar year.

## 2.10 Breach Notification to Office for Civil Rights (OCR)

45 CFR section 164.404 discusses breach reporting requirements for both large and small breaches.

For breaches of 500 or more individuals, notification will be made to the U.S. Department of Health and Human Services, Office for Civil Rights, as soon as notification is made to the individuals within 60 days.

Breaches of less than 500 will be maintained in a log and will be submitted no later than 60 days after the end of the calendar year in which the breaches were discovered.

### **Procedure**

OCR has created an online reporting tool that is available at this URL:

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruc tion.html>.

(A listing of regional OCR offices is available at this URL:  
<http://www.hhs.gov/ocr/office/about/rgn-hqaddresses.html>)

Reporting to the Department of Health and Human Services, Office for Civil Rights is done electronically at the URL noted above. The following are required data fields:

- Breach start date
- Discovery start date
- Type of breach
- Location of breached information (such as laptop computer, email, etc.)
- Type of breached information (such as demographic, clinical, financial, and other)
- Description of the breach
- Types of safeguards in place prior to breach (such as firewalls, anti-virus software, etc.)

## 2.11 Breach Notification to States

Many states now have data breach laws. Because health care organizations capture the kind of personal information that is the focus of these laws, reporting to states may be required. But not all states require reporting. If an individual lists a place of residence in a state that requires separate reporting, EHN shall comply with the requirements of said state law.

Emergence Health Network will comply with all state reporting requirements governing disclosures of individuals' personal information.

### **Procedure**

Emergence Health Network will report breaches to HHS contract manager and OCR at <https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf>.

## 2.12 Breach Notification Law Enforcement Delay

HIPAA rules (45 CFR section 164.404) allow for a delay in notifying individuals subject to a breach. Presumably both local and federal law enforcement may request a delay

HIPAA rules allow law enforcement to request a delay in informing individuals about breaches of protected health information.

### **Procedure**

Any delay in reporting a breach as requested by law enforcement will be documented using the form below.

**Breach Documentation for Law Enforcement**

Date of breach \_\_\_\_\_

Date of breach discovery \_\_\_\_\_

Number of individuals affected \_\_\_\_\_

Description of breach \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Law enforcement official requesting delay \_\_\_\_\_

Term of delay \_\_\_\_\_

Reason for delay \_\_\_\_\_

---

# Section 3—Conducting Internal HIPAA Audits

This section contains policies and procedures related to internal auditing.

## 3.1 Deciding What Information to Audit

With so many standards and rules, deciding what to audit may seem challenging. Any area that the organization has experienced issues within the past (e.g., data breach, lost or stolen laptop) is a good place to start. Another place to get ideas is the Office for Civil Rights (OCR), which oversees enforcement of the rules. Beginning in 2012, the OCR has begun mandatory auditing of covered entities (CE) and their HIPAA compliance programs. The focus of these audits and their findings are public information and should be reviewed to determine where to focus auditing efforts.

In an effort to bolster compliance and uncover any noncompliant areas Emergence Health Network will conduct regular audits of policies and procedures in place regarding the HIPAA compliance program. The focus of these audits will be determined by the Administrative Director of Health Information.

### **Procedure**

The Administrative Director of Health Information will determine where to focus audits based on complaints/grievances investigated in the past and input from leadership executives and/or managers who have concerns about specific areas. The Administrative Director of Health Information will also review audit emphasis and findings from the OCR to determine areas to focus auditing efforts.

## 3.2 Audit Plan

Developing a plan for each audit helps keep the audit on track, eliminate time wasted, and maintain focus in the specific areas outlined.

Each audit conducted by Emergence Health Network, whether triggered or periodic, will begin with development of a written audit plan.

### **Procedure**

Once the Administrative Director of Health Information has determined what areas or standards will be audited, the Administrative Director of Health Information will develop a written audit plan.

At a minimum each audit plan will include:

- Objective or purpose of the audit
- What will be audited
- Who will conduct the audit
- How the audit will be conducted (manually or automated)
- Resources utilized to conduct the audit

- Frequency of the audit (e.g., annually, semiannually, quarterly)

### 3.3 Conducting the Audit

Internal HIPAA audits by Emergence Health Network Associates will be conducted only once an audit plan is developed and the Administrative Director of Health Information has verified that all the appropriate information from available resources needed to conduct an accurate and thorough audit have been assembled.

If the Administrative Director of Health Information is conducting a routine audit and an unexpected event occurs, such as a mental health professional misplacing a laptop, the Administrative Director of Health Information may suspend the audit for a short period of time to tend to the more urgent matter. When conducting a triggered audit, the Administrative Director of Health Information and management should determine which event is higher priority.

#### **Procedure**

Any Associates conducting an audit of the privacy and/or security rules will follow the audit plan outlined by the Administrative Director of Health Information. The Administrative Director of Health Information will work with various entities (e.g., IT Associates, EHR vendor) to verify that all data required to conduct a thorough audit of a particular compliance area have been reported and are available to the auditor.

For more details on the actual audit process see **section 3.5**.

### 3.4 Reporting Audit Findings

For an audit program to be beneficial to Emergence Health Network, audit results should always be communicated to the appropriate department(s) and/or Associates.

Once an audit is completed the Administrative Director of Health Information, along with the auditor if someone other than the Administrative Director of Health Information, will submit the findings and recommendations for any corrective actions in a written report to the supervisor/manager of the department or Associates that was the subject of the audit.

The final report should include, at a minimum, the following:

- Date
- Subject
- Scope
- Dates reviewed in the audit
- Audit type (e.g., routine)
- Auditor
- Standard(s) addressed by the audit
- Resources used (attach copies to final report, include a storage device with the report, or place on a secure network)

- Findings or summary
- Recommendations
- Assignments (if corrective action is required)
- Follow-up

### Procedure

The Administrative Director of Health Information will ensure that the preliminary final report of the audit findings is complete, accurate, and is forwarded to the appropriate supervisor/manager for review. Once the supervisor/manager reviews the report, he or she may challenge the findings or corrective actions, present different data, or offer a different analysis. Any challenges to the findings are submitted directly to the Administrative Director of Health Information in writing. The original auditor, if other than the Administrative Director of Health Information, and the Administrative Director of Health Information will review any challenges.

At this point, there are only two solutions:

1. If the reviewer's comments are valid, the Administrative Director of Health Information will change the preliminary report.
2. The auditor verifies his or her own data, and if satisfied with the data collected, the auditor may reject the reviewer's analysis.

Whichever conclusion is reached, a final report is created and submitted to leadership and/or other management as appropriate to implement any needed corrective actions.

**Note:** Any disagreements, even if rejected by the Administrative Director of Health Information, should be documented in the final report.

## Final Report Template

<b>Report Date:</b>	<b>Auditor:</b> Privacy Officer	<b>Reviewed by:</b>
<b>Subject:</b>	<b>Dates reviewed:</b>	
<b>Scope:</b>	<b>Audit type (Circle one):</b> Routine or Triggered Event	
<b>Standard(s):</b>		
<b>Resource(s):</b>		
<b>Finding(s):</b>		

<b>Recommendation(s):</b>
<b>Assignment(s):</b>
<b>Follow-up:</b>
<b>Final report submitted to the CEO on:</b>

### 3.5 Privacy and Security Auditing

According to the OCR, about 60 percent of its initial audit findings are related to the security rule and 30 percent to the privacy rule. Incomplete policies and procedures for these specific areas contributed to the inadequacy of the programs audited.

Areas of the HIPAA compliance program within Emergence Health Network will be audited on a regular scheduled basis. These will include areas deemed high risk by the Administrative Director of Health Information, issues discovered based on complaints, grievances, and management/associate observations, and areas of focus and findings stemming from the OCRs auditing program.

#### **Procedure**

The Administrative Director of Health Information, or other Associates designated by the Administrative Director of Health Information or executive leadership, shall complete a thorough audit of information gathered based on the criteria listed in the finalized audit plan. The auditor will review the information as outlined in the plan (e.g., reports, logs, etc.), for compliance with existing policies and procedures in the HIPAA compliance program.

Most subjects or standards audited have specific criteria to be verified; therefore, the auditor(s) should follow the audit template(s) developed by the Administrative Director of Health Information. An auditor who deems that additional criteria should be added, or revisions made to an audit form should discuss with the Administrative Director of Health Information before altering the form. If collectively a decision is made to revise the form, any old forms should be disposed of and the updated form should include the date of revision.

---

# Section 4—Unique Identifier Policies and Procedures

This section contains policies and procedures related to the various regulations governing the use of unique identifiers.

## 4.1 Consumer Identifiers

As consumers change third-party payers on a regular basis, it is important their identifying information is verified on a regular basis. It is the procedure of Emergence Health Network that we will verify consumer insurance identifiers on at least an annual basis.

### **Procedure**

We will verify the insurance information of each consumer annually, including consumer ID number.

- The consumer will be asked to verify identifying information via a visual check of the consumer information form kept in the chart.
- The consumer will be asked to present an insurance card.
- A copy of the insurance card will be kept with the consumer's other billing information.
- The consumer will be asked about any possible secondary insurance or other pertinent identifying information the practice needs.

These reviews will occur starting each January and completed reviews will be noted in the chart and in the master consumer index online to avoid requesting the same information from the consumer twice.

## 4.2 Provider Identifiers

Emergence Health Network will require that associates identified as health care providers and organization clinics identified as covered entities obtain a national provider identifier (NPI).

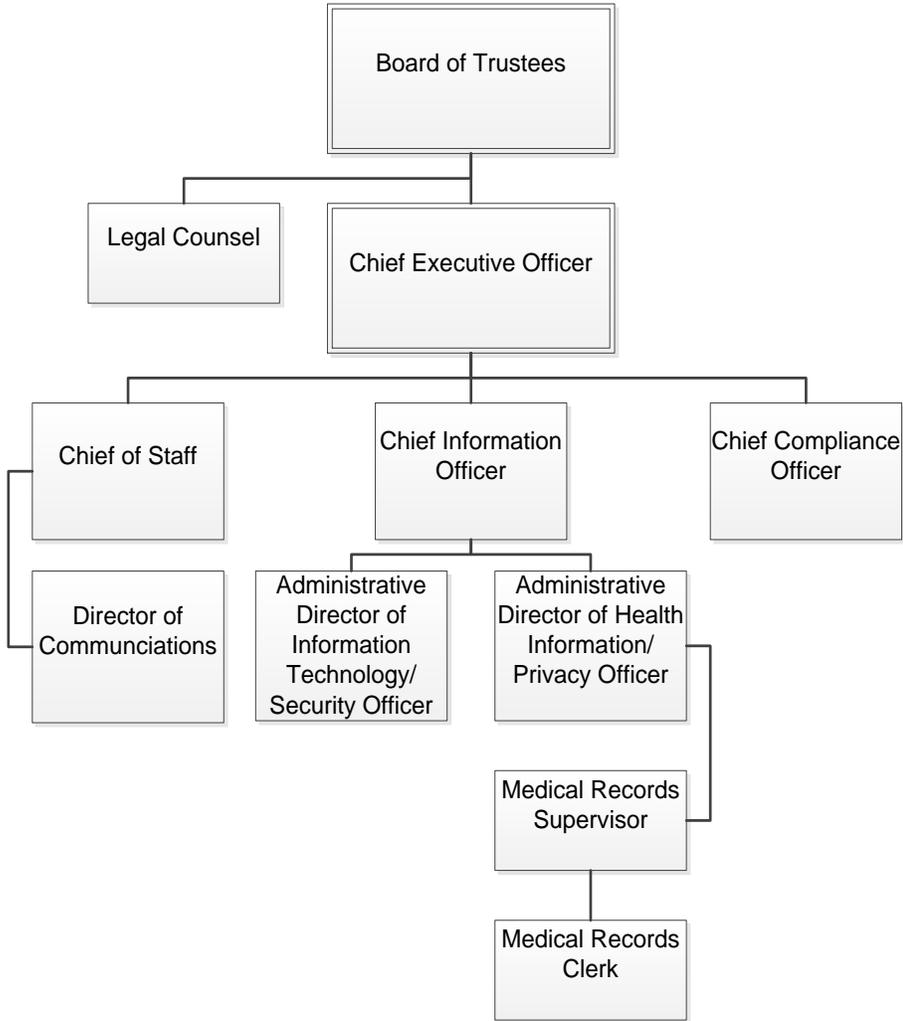
### **Procedure**

Emergence Health Network will verify that all providers it employs have the appropriate national provider identifier (NPI) number. Any provider who does not yet have an NPI number will apply for one through the enumerator site at <https://nppes.cms.hhs.gov/NPPES/Welcome.do>.

If changes need to be made to the information on a provider's NPI record, such as address, phone number, affiliation, etc., Emergence Health Network will contact the enumerator to provide that information.

# Appendix A— Privacy Forms

EHN Privacy Policy Organizational Chart



**LIST OF PRIVACY RELATED POSITIONS**

<b>Title of Position</b>	<b>Name of Employee</b>
Chief Executive Officer	Kristi Daugherty
Legal Counsel	Michael Wyatt
Legal Counsel	Anthony Martinez
Chief Information Officer	Juan Gonzalez
Administrative Director of Health Information	Orlando Gonzalez
Administrative Director of Information Technology	Ana Matos
Medical Records Supervisor	Arlene Gallardo
Chief Compliance Officer	Rene Navarro
Chief of Staff	Rene Hurtado
Director of Communications	Noreen Jaramillo

## SAMPLE BUSINESS ASSOCIATE AGREEMENT

**THIS BUSINESS ASSOCIATE AGREEMENT** (“BA Agreement”) is made effective as of \_\_\_\_\_ (“Effective Date”), by and between El Paso MHMR d/b/a Emergence Health Network (“Covered Entity”), and \_\_\_\_\_, (“Business Associate”). Covered Entity and Business Associate may be referred to in this BA Agreement as a “Party” individually and as “Parties” collectively.

### RECITALS

**WHEREAS**, Business Associate has a relationship with Covered Entity under a certain agreed arrangement (the “Service Agreement”) in which Business Associate provides services to Covered Entity (the “Services”) and in which Business Associate is entrusted with confidential, individually identifiable patient information (“Protected Health Information” or “PHI”), which Business Associate may access, create, and use in providing the Services to Covered Entity and which is otherwise protected by state or federal law.

**WHEREAS**, both Parties desire to meet their obligations to protect PHI under: (i) the Standards for Privacy of Individually Identifiable Health Information (“Privacy Rule”) and the Security Standards (“Security Rule”) published by the U.S. Department of Health and Human Services (“DHHS”) at 45 CFR parts 160 through 164 under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”); and (ii) the additional Privacy and Security Rule requirements pursuant to Subtitle D of the Health Information Technology for Economic and Clinical Health Act (“HITECH”), including 45 CFR Sections 164.308, 164.310, 164.312, and 164.316, as amended from time to time.

**WHEREAS**, both Parties further desire to meet their obligations to protect PHI under additional privacy and security requirements adopted by the Texas Legislature, which apply equally to business associates as “covered entities” under Texas law and may be more restrictive than those required under HIPAA and HITECH.

**WHEREAS**, both Parties desire to make technical and procedural arrangements to assure that their business relationships meet each of these various statutory or regulatory requirements.

**WHEREAS**, both Parties desire to set forth the terms and conditions pursuant to which PHI that is provided by, or created or received by, Business Associate on behalf of Covered Entity will be handled between themselves and third parties.

**NOW THEREFORE**, in consideration of the foregoing and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties hereby agree as follows:

**Definitions.** Regulatory citations in this BA Agreement are to the United States Code of Federal Regulations (“CFR”), as promulgated, interpreted, and amended from time to time by DHHS, for so long as such regulations are in effect. Unless otherwise specified in this BA Agreement, all terms not otherwise defined shall have the meaning established for purposes of parts 160 through 164 of Title 45 of the CFR, as amended from time to time.

### Permitted Uses and Disclosures of PHI

**Services.** Covered Entity and Business Associate have an indirect business relationship whereby Business Associate will provide the Services to Covered Entity that may involve the use or disclosure of PHI. The Services will be provided to Covered Entity under the Service Agreement that specifies the Services to be provided by Business Associate to or on behalf of Covered Entity.

**Use of PHI.** As specified in this BA Agreement, Business Associate may use or disclose PHI created or received from or on behalf of Covered Entity necessary to perform its obligations under the Service Agreement; provided, however, that all other uses not authorized by this BA Agreement, the applicable subcontract, the applicable Service Agreement, or other written instructions from the Covered Entity, are prohibited. Moreover, Business Associate may disclose PHI for the purposes authorized by this BA Agreement only: (i) to its employees,

subcontractors, and agents in accordance with Section 3.1(h) below; (ii) as directed by Covered Entity; or (iii) as otherwise permitted by the terms of this BA Agreement.

**Data Analysis.** Deleted.

**Business Activities of Business Associate.** Unless otherwise limited in this BA Agreement, Business Associate may:

Use the PHI in its possession for its proper management and administration and to fulfill any present or future legal responsibilities of Business Associate;

Disclose the PHI in its possession to third parties for the purpose of its proper management and administration or to fulfill any present or future legal responsibilities of the Business Associate, provided that: (i) the disclosures are “required by law,” as defined in 45 CFR § 164.501; (ii) the disclosures do not require an authorization or “opportunity to agree” as defined in 45 CFR § 164.512; or (iii) Business Associate has received from the third party written assurances regarding its confidential handling of such PHI as required under 45 CFR § 164.308(b)(1) and 45 CFR §164.504(e)(4);

(c) De-identify any and all PHI provided that Business Associate implements de-identification criteria in accord with 45 CFR § 164.514(b) and further provided that Business Associate provides to Covered Entity the documentation required by 45 CFR § 164.514(b), which may be in the form of a written assurance from the Business Associate. De-identified information does not constitute PHI and is not subject to the terms of this BA Agreement; provided, however, absent prior written authorization from Covered Entity, such de-identified information shall not include business, proprietary, or other information about Covered Entity;

Make uses and disclosures and requests for PHI consistent with Covered Entity’s minimum necessary policies and procedures;

Business Associate may disclose PHI to Covered Entity in accordance with its Service Agreement to perform its obligations to Covered Entity; and

## **Responsibilities of the Parties With Respect to PHI.**

**Responsibilities of the Business Associate.** With regard to its use or disclosure of PHI, the Business Associate shall:

Use or disclose the minimum amount of PHI necessary as permitted or required by this BA Agreement or as otherwise required by law to accomplish the intended purpose of such use or disclosure;

Develop and maintain a comprehensive written health information privacy and security program that implements: (i) appropriate policies, procedures, and protections as required by the Privacy Rule for the privacy of PHI; (ii) appropriate Administrative (45 CFR § 164.308), Physical (45 CFR § 164.310), and Technical (45 CFR § 164.312) Safeguards (collectively, the “Safeguards”) that reasonably protect PHI, including electronic PHI (“e-PHI”), as required by the Security Rule and amended from time to time; and (iii) appropriate policies, procedures, and protections to implement and document such Safeguards as required by 45 CFR § 164.316;

To the extent feasible, use commercially reasonable efforts to secure PHI through technology standards that render such PHI unusable, unreadable, and indecipherable to individuals unauthorized to acquire or otherwise have access to such PHI in accordance with guidance published by DHHS at 74 Federal Register 19006 (April 17, 2009), or such later regulations or guidance promulgated by DHHS or issued by the National Institute for Standards and Technology (“NIST”) concerning the protection of identifiable data such as PHI;

Report to the designated Privacy Officer of Covered Entity, in writing, any use or disclosure of PHI that is not permitted or required by this BA Agreement of which Business Associate becomes aware no more than

48 hours of Business Associate's discovery of such unauthorized use or disclosure;

Establish procedures for mitigating, to the greatest extent possible, any harmful effects from any improper use or disclosure of PHI that Business Associate knows of and reports to Covered Entity as referenced in Section 3.1(d) above;

Report to the designated Security Officer of Covered Entity, in writing, any breach in the security, confidentiality, integrity, or availability of e-PHI that Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity of which Business Associate becomes aware no more than 48 hours of Business Associate's discovery of such security breach;

Establish procedures for mitigating, to the greatest extent possible, any harmful effects from any improper breach to the security, confidentiality, integrity, or availability of e-PHI that Business Associate knows of and reports to Covered Entity as referenced in Section 3.1(f) above;

In accordance with Section 3.3 of this BA Agreement, notify the Privacy and Security Officer of Covered Entity no later than 48 hours after which Business Associate knows, or through exercise of reasonable diligence would have known, of any breach of Unsecured PHI (as defined by HITECH) accessed, maintained, retained, modified, recorded, stored, destroyed, or otherwise, held, used, or disclosed by Business Associate;

Require all its subcontractors and agents that receive, use, or have access to PHI under this BA Agreement, to sign a written agreement that:

Binds such subcontractors and agents to the same restrictions and conditions that apply to Business Associate pursuant to this BA Agreement as to the use or disclosure of PHI or the security, confidentiality, integrity, and availability of PHI;

Requires such subcontractors and agents to provide adequate safeguards against improper use or disclosure or breach of security related to e-PHI;

Contains reasonable assurances from such subcontractors and agents that the PHI they hold or maintain will remain confidential as provided in this BA Agreement and only disclosed as provided in this BA Agreement or required by law for the purposes for which it was disclosed to the respective subcontractor or agent; and

Obligates such subcontractors and agents to immediately notify Business Associate of any breaches of the confidentiality of PHI, including any security breach of Unsecured PHI, to the extent the respective subcontractor or agent obtains knowledge of such a breach.

Make available all records, books, agreements, policies, and procedures relating to the use or disclosure of PHI to the Secretary of DHHS for purposes of determining Covered Entity's compliance with the Privacy Rule and the Security Rule;

Upon written request, make available within 10 business days make available the information required to provide an accounting of disclosures to the Covered Entity as necessary to satisfy the Covered Entity's obligations under 45 CFR 164.528;

As of the Effective Date, comply with the HITECH Standards, each as may be applicable to the Services provided by Business Associate to Covered Entity pursuant to this BA Agreement, including, but not limited to: (i) the prohibition of the sale of PHI without authorization, unless an exemption under HITECH § 13405(d) applies; (ii) the prohibition on receiving remuneration (directly or indirectly from individuals) for certain communications that fall within the exceptions to the definition of marketing under 45 CFR § 164.501, unless permitted by this BA Agreement and HITECH § 13406; and (iii) the requirements regarding accounting of certain disclosures of PHI maintained in an electronic health record under HITECH § 13405(c)

Not: (i) sell PHI in such a way as to violate Section 181.153 of the Texas Health and Safety Code ("H&S

Code”), as amended by HB 300 (82<sup>nd</sup> Legislature; effective as of September 1, 2012) or further amended from time to time; (ii) use PHI in such a manner as to violate Section 181.152 of the H&S Code, or (iii) attempt to re-identify any information in violation of Section 181.151 of the H&S Code, regardless of whether such action is on behalf of or permitted by Covered Entity; and

Subject to Section 5.5 below, return to Covered Entity or destroy, within 90 days of the termination of this BA Agreement, the PHI in its possession and retain no copies (which for purposes of this BA Agreement shall mean segregable databases, files, or recording media identifiable to Covered Entity that are used by Business Associate in providing Services on behalf of Covered Entity).

**Responsibilities of the Covered Entity.** With regard to the use or disclosure of PHI by Business Associate, Covered Entity shall:

Obtain any consent or authorization that may be required by 45 CFR § 164.506 and 45 CFR § 164.508, or applicable state law, prior to furnishing Business Associate the PHI pertaining to an individual

Notify Business Associate of any limitations in Covered Entity’s notice of privacy practices in accordance with 45 CFR § 164.520 to the extent that such limitation may affect Business Associate’s use or disclosure of PHI; and

Not furnish Business Associate PHI that is subject to any arrangements permitted or required of Covered Entity under 45 CFR parts 160 through 164 that may impact in any manner the use or disclosure of PHI by Business Associate under this BA Agreement and the Service Agreement, including, but not limited to, restrictions on use or disclosure of PHI as provided for in 45 CFR § 164.522 and agreed to by Covered Entity.

**Responsibilities of the Parties with Respect to Breach Notification.** Covered Entity and Business Associate will comply with HITECH § 13402 and any regulations implementing such provisions, currently Subpart D of Title 45 of the CFR, as such regulations may be in effect from time to time (collectively, the “Breach Notification Rules”).

Except as provided by 45 CFR § 164.412, Business Associate will give Covered Entity notice of any breach of Unsecured PHI without unreasonable delay and in no event later than 48 hours after Business Associate discovered such breach. For purposes of reporting a breach to Covered Entity, the discovery of such a breach will be deemed to occur as of the first day on which Business Associate knows or, by exercising reasonable diligence, should have known of such breach. Business Associate will be deemed to have knowledge of such a breach if it is known, or by exercising reasonable diligence should have been known, by any person (other than the person committing the breach) who is an employee, director, officer, or other agent of Business Associate.

More specifically and for purposes of this BA Agreement, a “breach” is an unauthorized acquisition, access, use, or disclosure of Unsecured PHI, which compromises the security or privacy of the PHI. A breach compromises the privacy or security of the PHI if it poses a significant risk of financial, reputational, or other harm to the individual whose PHI was compromised.

Upon discovery and within the time limits set forth in this Section 3.3, Business Associate shall notify Covered Entity of a breach of Unsecured PHI with sufficient information to allow compliance with the Breach Notification Rule. Such notice will be written in plain language and will include, to the extent possible or available, the following:

the identification and contact information of all individuals whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during the breach;

a brief description of what happened, including the date of the breach and the date of the discovery of the breach;

a description of the types of Unsecured PHI that were involved in the breach;

any steps that individuals who were subjects of the breach should take to protect themselves from potential harm that may result from the breach;

a brief description of what Business Associate is doing to investigate the breach, to mitigate the harm to affected individuals, and to protect against further breaches; and

contact procedures for affected individuals to ask questions or learn additional information, including a toll-free telephone number, an email address, a website, or postal address.

Notwithstanding the provisions of this Section 3.3 and if a law enforcement official states to Business Associate that notification of a breach would impede a criminal investigation or cause damage to national security, then: (i) the notification shall be delayed for the time period specified by the official if the official's statement is in writing and specifies the time for which a delay is required; or (ii) if the official's statement is made orally, Business Associate shall document the oral statement, including the identity of the official making the statement, and delay the breach notification for no longer than 30 days from the date of the oral statement, unless the official submits a written statement during that time period.

The party responsible for the breach of Unsecured PHI shall be responsible for payment of all actual costs associated with the breach, including, but not limited to, costs of notifying affected individuals, credit monitoring (where applicable), and other efforts to mitigate the harm to affected individuals.

**Responsibilities of the Parties with Respect to Designated Record Sets.** This Section 3.4 applies only if, in the course of performing the Services, Business Associate and Covered Entity agree that Business Associate will maintain Designated Records Sets containing PHI. As such:

Business Associate shall: (i) at the request of, and in the time and manner designated by Covered Entity, provide access to the PHI to Covered Entity, or the individual to whom such PHI relates, or his or her authorized representative, in order to satisfy a request by such individual under HIPAA; and (ii) at the request of, and in the time and manner designated by Covered Entity, make any amendment(s) to the PHI that Covered Entity directs.

Covered Entity shall: (i) notify Business Associate, in writing, of any PHI that Covered Entity seeks to make available to an individual pursuant to HIPAA and will cooperate with Business Associate as to the time, manner, and form in which Business Associate shall provide such access; and (ii) notify Business Associate, in writing, of any amendment(s) to the PHI in the possession of Business Associate that Covered Entity believes is necessary because of its belief that the PHI that is the subject of the amendment(s) has been or could be relied upon by Business Associate or others to the detriment of the individual who is the subject of the PHI.

**Representations and Warranties of the Parties.** Each Party represents and warrants to the other Party:

**Workforce Informed of BA Agreement Terms.** All of the Parties employees, agents, representatives, and members of its respective workforce, whose services may be used to fulfill obligations under this BA Agreement are or shall be appropriately informed of the applicable terms of this BA Agreement and are under legal obligation to each Party, respectively, by contract or otherwise, sufficient to enable each Party to fully comply with all applicable provisions of this BA Agreement.

**Reasonable Cooperation among Parties.** Each Party will reasonably cooperate with the other Party in the

performance of the mutual obligations under this BA Agreement.

### **Term and Termination.**

**Term.** This BA Agreement shall become effective on the Effective Date and shall continue in effect unless terminated as provided in this Article 5. In addition, certain provisions and requirements of this BA Agreement shall survive the expiration or termination of this BA Agreement in accordance with Section 6.6 below.

**Termination by Covered Entity.** As provided under 45 CFR § 164.314(a)(2)(i) and 45 CFR § 164.504(e)(2)(iii), Covered Entity may immediately terminate this BA Agreement and any related Service Agreement if Covered Entity makes the determination that the Business Associate has breached a material term of this BA Agreement. Alternatively, Covered Entity may choose to: (i) provide the Business Associate with 7-days' prior 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. Nonetheless, in the event that mutually agreeable terms cannot be achieved within 30 days, Business Associate must cure said breach to the satisfaction of Covered Entity within 90 days. Failure to cure in the manner set forth in this Section 5.2 shall be grounds for the immediate termination of this BA Agreement and any related Service Agreements.

**Termination by Business Associate.** Business Associate may immediately terminate this BA Agreement and any related Service Agreements if Business Associate makes the determination that Covered Entity has breached a material term of this BA Agreement. Alternatively, Business Associate may choose to: (i) provide Covered Entity with 7-days' prior written notice of the existence of an alleged material breach; and (ii) afford Covered Entity an opportunity to cure said alleged material breach upon mutually agreeable terms. Nonetheless, in the event that mutually agreeable terms cannot be achieved within 90 days, Covered Entity must cure said breach to the satisfaction of Business Associate within 90 days. Failure to cure in the manner set forth in this Section 5.3 shall be grounds for the immediate termination of this BA Agreement.

**Automatic Termination.** This BA Agreement will automatically terminate without any further action of the Parties upon the termination or expiration for whatever reason of all Service Agreement(s) between Covered Entity and Business Associate to which any subcontract between Business Associate and Contractor, or any sooner termination or expiration for whatever reason of all subcontracts between Business Associate and Contractor relating to any Service Agreement.

**Effect of Termination.** Upon the termination of this BA Agreement pursuant to this Article 5, Business Associate shall return or destroy within 90 days all PHI, including e-PHI, identifiable to Covered Entity, including such information in possession of Business Associate's subcontractors, if it is feasible to do so. If return or destruction of said PHI is not feasible, the Business Associate shall notify the Covered Entity in writing. Said notification shall include: (i) a statement that Business Associate has determined that it is not feasible to return or destroy the PHI in its possession; and (ii) the specific reasons for such determination. In the event Business Associate determines that the return or destruction of said PHI is not feasible and has provided proper written verification to Covered Entity of this determination as prescribed in this Section 5.5, Business Associate shall extend any and all protections, limitations, and restrictions contained in this BA Agreement to Business Associate's use or disclosure of any PHI retained after the termination of this BA Agreement, and to limit any further uses or disclosures to the purposes that make the return or destruction of the PHI infeasible.

### **Miscellaneous.**

**Rights of Proprietary Information.** Covered Entity retains any and all rights to the proprietary information, confidential information, and PHI it releases to Business Associate.

**Nature of Agreement; Independent Contractors.** Nothing in this BA Agreement shall be construed to create an employer-employee relationship or partnership, joint venture, or other joint business relationship between the Parties or any of their affiliates. Business Associate is an independent contractor, and not an agent, of Covered

Entity. This BA Agreement does not express or imply any commitment to purchase or sell goods or services.

**ENTIRE AGREEMENT.** THIS BA AGREEMENT CONSTITUTES THE ENTIRE AGREEMENT OF THE PARTIES WITH RESPECT TO THE PARTIES' COMPLIANCE WITH FEDERAL OR STATE HEALTH INFORMATION CONFIDENTIALITY LAWS AND REGULATIONS, AS WELL AS THE PARTIES' OBLIGATIONS UNDER THE BUSINESS ASSOCIATE PROVISIONS OF 45 CFR PARTS 160 THROUGH 164. THIS BA AGREEMENT SUPERSEDES ALL PRIOR OR CONTEMPORANEOUS WRITTEN OR ORAL MEMORANDA, ARRANGEMENTS, CONTRACTS, OR UNDERSTANDINGS BETWEEN THE PARTIES RELATING TO THE PARTIES' COMPLIANCE WITH FEDERAL OR STATE HEALTH INFORMATION CONFIDENTIALITY LAWS AND REGULATIONS AND THE PARTIES' HEALTH INFORMATION CONFIDENTIALITY AND SECURITY OBLIGATIONS UNDER 45 CFR PARTS 160 THROUGH 164 OR APPLICABLE STATE LAW.

**Change of Law.** Covered Entity shall notify Business Associate within 90 days of any amendment to any provision of state or federal law which materially alters either Party's or both Parties' obligations under this BA Agreement. Upon provision of such notice by Covered Entity to Business Associate, the Parties shall negotiate in good faith mutually acceptable and appropriate amendment(s) to this BA Agreement to give effect to such revised obligations; provided, however, that if the Parties are unable to agree on mutually acceptable amendment(s) within 90 days of the relevant change of law, either Party may terminate this BA Agreement consistent with Sections 5.5 and 6.6 herein.

**Construction of Terms.** The terms of this BA Agreement shall be construed in light of any interpretation or guidance on HIPAA, HITECH, the Privacy Rule, or the Security Rule issued by DHHS from time to time. Furthermore, any ambiguity in this BA Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule and Security Rule.

**GOVERNING LAW.** IN THE EVENT THE LAWS OF THE STATE OF TEXAS PROVIDE MORE STRINGENT PROTECTION OF PHI THAN HIPAA OR IN THE EVENT OF A STATE LAW DISPUTE BETWEEN THE PARTIES, THE INTERPRETATION AND ENFORCEMENT OF THIS BA AGREEMENT SHALL BE CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF TEXAS. EXCLUSIVE VENUE FOR A CAUSE OF ACTION FOR SUCH A STATE LAW DISPUTE SHALL BE IN A COURT OF COMPETENT JURISDICTION IN EL PASO COUNTY, TEXAS.

**Survival.** This Section 6.6 shall survive termination of this BA Agreement for any reason. Further, the respective rights and obligations of Business Associate and Covered Entity under the provisions of Sections 3.1, 3.2, 3.3, and 5.5 above, solely with respect to PHI Business Associate retains in accordance with Section 5.5 above, shall survive the expiration or termination of this BA Agreement for so long as such PHI is retained by Business Associate.

**Amendment: Waiver.** This BA Agreement may not be modified, nor shall any provision of this BA Agreement be waived or amended, except in a writing duly signed by authorized representatives of the Parties. A waiver with respect to one event shall not be construed as continuing or as a bar to or waiver of any right or remedy as to subsequent events.

**Assignment of Rights and Delegation of Duties.** This BA Agreement is binding upon and inures to the benefit of the Parties and their respective successors and permitted assigns. However, neither Party may assign any of its rights or delegate any of its obligations under this BA Agreement without the prior written consent of the other Party, which consent shall not be unreasonably withheld or delayed. Notwithstanding any provisions herein to the contrary, Covered Entity retains the right to assign or delegate any of its rights or obligations in this BA Agreement to any of its wholly owned subsidiaries, affiliates, or successor companies. Assignments made in violation of this Section 6.8 shall be null and void.

**Equitable Relief.** Any use, disclosure, or breach of privacy or security of PHI by Business Associate in violation of this BA Agreement will cause Covered Entity irreparable harm, the amount of which may be difficult to ascertain. Business Associate therefore acknowledges and agrees that Covered Entity shall have the right to apply to a court of competent jurisdiction for specific performance and/or an order restraining and enjoining Business Associate from any such further use, disclosure, or breach, and for such other relief as Covered Entity shall deem appropriate.

Such rights are in addition to any other remedies available to Covered Entity at law or in equity.

**Severability.** The provisions of this BA Agreement are severable, and if any provision of this BA Agreement shall be held or declared to be illegal, invalid, or unenforceable, the remainder of this BA Agreement shall continue in full force and effect as though such illegal, invalid, or unenforceable provision had not been contained in this BA Agreement.

**No Third-Party Beneficiaries.** Nothing in this BA Agreement is intended to confer on any person other than the Parties, or their respective successors and assigns, any rights, remedies, obligations, or liabilities under or by reason of this BA Agreement. Nothing in this BA Agreement shall be considered or construed as conferring any right or benefit on a person not party to this BA Agreement nor imposing any obligations on either Party hereto to persons not a party to this BA Agreement.

**Notices.** Any notices to be given hereunder to a Party shall be made via U.S. Mail or express courier to the appropriate Party as follows:

**COVERED ENTITY:**

El Paso MHMR d/b/a  
Emergence Health Network  
Attn: Privacy Officer  
201 East Main, Suite 600  
El Paso, Texas 79901

**BUSINESS ASSOCIATE:**

\_\_\_\_\_

Each Party may change its address and that of its representative for notice by the giving of notice thereof in the manner herein provided.

**Counterparts; Facsimiles.** This BA Agreement may be executed in any number of counterparts, each of which shall be deemed an original. Facsimile copies hereof shall be deemed to be originals.

**Disputes.** If any controversy, dispute, or claim arises between the Parties with respect to this BA Agreement, the Parties shall make good faith efforts to resolve such matters informally.

**IN WITNESS WHEREOF,** each of the undersigned has caused this BA Agreement to be duly executed in its name and on its behalf effective as of the Effective Date.

**COVERED ENTITY:**

**El Paso MHMR d/b/a  
Emergence Health Network**

By: \_\_\_\_\_  
Kristen Daugherty  
Chief Executive Officer

Date: \_\_\_\_\_

**BUSINESS ASSOCIATE:**

\_\_\_\_\_

By: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

## Notice of Privacy Practices

### **EL PASO MHMR D/B/A EMERGENCE HEALTH NETWORK (“EHN”) - NOTICE OF PRIVACY PRACTICES (“NPP”) 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**

For purposes of this Notice “us” “we” and “our” refers to EHN: and “you” or “your” refers to our consumers (or their legal representatives as determined by us in accordance with state informed consent law). When you receive healthcare services from us, we will obtain access to your medical information (i.e. your health history). We are committed to maintaining the privacy of your health information and we have implemented procedures to ensure that we do so.

The Federal Health Insurance Portability & Accountability Act of 2013, HIPAA Omnibus Rule, (formally HIPAA 1996 & HITECH of 2004) require us to maintain the confidentiality of all your healthcare records and other identifiable consumer health information (PHI) used by or disclosed to us in any form, whether electronic, on paper, or spoken. HIPAA is a Federal Law that gives you significant new rights to understand and control how your health information is used. Federal and state law provide penalties for covered entities, Business Associates, and their subcontractors and records owners, respectively that misuse or improperly disclose PHI.

Starting April 14, 2013, HIPAA requires us to provide you with the Notice of our legal duties and the privacy practices we are required to follow when you first come into our office for health-care services. If you have any questions about this Notice, please ask to speak to our HIPAA Privacy Officer. Our doctors, clinical staff, employees, Business Associates (outside contractors we hire), their subcontractors and other involved parties follow the policies and procedures set forth in this Notice.

We are required to give you this notice of our legal duties and privacy practices, and we must do what this notice says. We will ask you to sign an acknowledgement that you have received this notice. We can change the contents of this notice and, if we do, we will have copies of the new notice at our facilities and on our website: <http://emergencehealthnetwork.org>

**WE MAY USE AND DISCLOSE YOUR PROTECTED HEALTH INFORMATION.** Under the law, we must have your signature on a written, dated consent form and/or an authorization form of acknowledgement of this notice, before we will use or disclose your PHI for certain purposes as detailed in the rules below. **Documentation** – You will be asked to sign an authorization / acknowledgement form when you receive this NPP. If you did not sign such a form or need a copy of the one you signed, please contact our Privacy Officer. You may take back or revoke your consent or authorization at any time (unless we already have acted based on it) by submitting our Revocation Form in writing to us at our address listed above. Your revocation will take effect when we actually receive it. We cannot give it retroactive effect, so it will not affect any use or disclosure that occurred in our reliance on your consent or authorization prior to revocation (i.e. if after we provide services to you, you revoke your authorization / acknowledgement in order to prevent us billing or collecting for those services, your revocation will have no effect because we relied on your authorization/ acknowledgement to provide services before you revoked it). **General Rule** – If you do not sign our authorization/ acknowledgement form or if you revoke it, as a general rule (subject to exceptions described below under “Healthcare Treatment, Payment and Operations Rule” and “Special Rules”), we cannot in any manner use or disclose to anyone (excluding you, but including payers and Business Associates) your PHI or any other information in your medical record. By law, we are unable to submit claims to payers under assignment of benefits without your signature on our authorization/ acknowledgement form. You will however be able to restrict disclosures to your insurance carrier for services for which you wish to pay “out of pocket”. We will not condition treatment on you signing an authorization / acknowledgement, but we may be forced to decline you as a new consumer or discontinue you as an active consumer if you choose not to sign the authorization/ acknowledgement or revoke it.

**Healthcare Treatment, Payment and Operations** With your signed consent, we may use or disclose your PHI in order: (1) To provide you with or coordinate healthcare treatment and services. For example, we may review your health history form to form a diagnosis and treatment plan, consult with other doctors about your care, delegate tasks to ancillary staff, call in prescriptions to your pharmacy, disclose needed information to your family or others so they may assist you with home care, arrange appointments with other healthcare providers, schedule lab work for you, etc. (2) To bill or collect payment from you, an insurance company, a managed-care organization, a health benefits plan or another third party. For example, we may need to verify your insurance coverage, submit your PHI on claim forms in order to get reimbursed for our services, obtain pre-treatment estimates or prior authorizations from your health plan or provide your x-rays because your health plan requires them for payment; Remember, you will be able to restrict disclosures to your insurance carrier for services for which you wish to pay “out of pocket”. (3) To run our office, assess the quality of care our consumers receive and provide you with customer service. For example, to improve efficiency and reduce costs associated with missed appointments, we may contact you by telephone, mail or otherwise remind you of scheduled appointments, we may leave messages with whomever answers your telephone or email to contact us (but we will not give out detailed PHI), we may call you by name from the waiting room, we may ask you to put your name on a sign-in sheet, (we will cover your name just after checking you in), we may tell you about or recommend health-related products and complementary or alternative treatments that may interest you, we may review your PHI to evaluate our staff’s performance, or our Privacy Officer may review your records to assist you with complaints. If you prefer that we not contact you with appointment reminders or information about treatment alternatives or health-related products and services, please notify us in writing at our address listed above and we will not use or disclose your PHI for these purposes. (4) HIPAA does not require that we provide the above notice regarding appointment reminders, treatment information or health benefits, but we are including these as a courtesy, so you understand our business practices with regards to your PHI. Additionally, you should be made aware of these protection laws on your behalf, under HIPAA: **Health insurance plans** that underwrite cannot use or disclose genetic information for underwriting purposes (this excludes certain long-term care plans). Health plans that post their NPPs on their web sites must post these Omnibus Rule changes on their sites by the effective date of the Omnibus Rule, as well as notify you by US Mail by the Omnibus Rules effective date. Plans that do not post their NPPs on their Web sites must provide you information about Omnibus Rule changes within 60 days of these federal revisions.

**Psychotherapy Notes** If we maintain psychotherapy notes on you, we can only allow use and disclosure of such notes with your written authorization.

**Special Rules** Notwithstanding anything else contained in this NPP, only in accordance with HIPAA, and under strictly limited circumstances, we may use or disclose your PHI without your permission, consent or authorization for the following purposes: **(1)** When required under federal, state or local law; **(2)** When necessary in emergencies to prevent a serious threat to your health and safety or the health and safety of other persons; **(3)** When necessary for public health reasons (i.e. prevention or control of disease, injury or disability, reporting information such as adverse reactions to anesthesia, ineffective or dangerous medications or products, suspected abuse, neglect or exploitation of children, disabled adults or the elderly, or domestic violence); **(4)** For federal or state government health-care oversight activities (i.e. civil rights laws, fraud and abuse investigations, audits, investigations, inspections, licensure or permitting, government programs, etc.); **(5)** For judicial and administrative proceedings and law enforcement purposes (i.e. in response to a warrant, subpoena or court order, by providing PHI to coroners, medical examiners and funeral directors to locate missing persons, identify deceased persons or determine cause of death); **(6)** For worker's compensation purposes (i.e. we may disclose your PHI if you have claimed health benefits for a work-related injury or illness); **(7)** For intelligence, counterintelligence or other national security purposes (i.e. Veterans Affairs, U.S. military command, other government authorities or foreign military authorities may require us to release PHI about you); **(8)** For organ and tissue donation (i.e. if you are an organ donor, we may release your PHI to organizations that handle organ, eye or tissue procurement, donation and transplantation); **(9)** For research projects approved by an Institutional Review Board or a privacy board to ensure confidentiality (i.e. if the researcher will have access to your PHI because involved in your clinical care, we will ask you to sign an authorization); **(10)** To create a collection of information that is "de-identified" (i.e. it does not personally identify you by name, distinguishing marks or otherwise and no longer can be connected to you); **(11)** To family members, friends and others, but only if you are present and verbally give permission. We give you an opportunity to object and if you do not, we reasonably assume, based on our professional judgment and the surrounding circumstances, that you do not object (i.e. you bring someone with you into the operatory or exam room during treatment or into the conference area when we are discussing your PHI); we reasonably infer that it is in your best interest (i.e. to allow someone to pick up your records because they knew you were our consumer and you asked them in writing with your signature to do so); or it is an emergency situation involving you or another person (i.e. your minor child or ward) and, respectively, you cannot consent to your care because you are incapable of doing so or you cannot consent to the other person's care because, after a reasonable attempt, we have been unable to locate you. In these emergency situations we may, based on our professional judgment and the surrounding circumstances, determine that disclosure is in the best interests of you or the other person, in which case we will disclose PHI, but only as it pertains to the care being provided and we will notify you of the disclosure as soon as possible after the care is completed.

**Minimum Necessary** Our staff will not use or access your PHI unless it is necessary to do their jobs (i.e. doctors uninvolved in your care will not access your PHI; ancillary clinical staff caring for you will not access your billing information; billing staff will not access your PHI except as needed to complete the claim form for the latest visit; janitorial staff will not access your PHI). All of our team members are trained in HIPAA Privacy rules and sign strict confidentiality contracts with regards to protecting and keeping private your PHI. So do our Business Associates and their subcontractors. Know that your PHI is protected several layers deep with regards to our business relations. Also, we disclose to others outside our staff, only as much of your PHI as is necessary to accomplish the recipient's lawful purposes. Still in certain cases, we may use and disclose the entire contents of your medical record: **(a)** To you (and your legal representatives as stated above) and anyone else you list on a consent or authorization to receive a copy of your records; **(b)** To healthcare providers for treatment purposes (i.e. making diagnosis and treatment decisions or agreeing with prior recommendations in the medical record); **(c)** To the U.S. Department of Health and Human Services (i.e. in connection with a HIPAA complaint); **(d)** To others as required under federal or state law; **(e)** To our privacy officer and others as necessary to resolve your complaint or accomplish your request under HIPAA (i.e. clerks who copy records need access to your entire medical record). In accordance with HIPAA law, we presume that requests for disclosure of PHI from another Covered Entity (as defined in HIPAA) are for the minimum necessary amount of PHI to accomplish the requestor's purpose. Our Privacy Officer will individually review unusual or non-recurring requests for PHI to determine the minimum necessary amount of PHI and disclose only that. For non-routine requests or disclosures, our Privacy Officer will make a minimum necessary determination based on, but not limited to, the following factors: **(a)** The amount of information being disclosed; **(b)** The number of individuals or entities to whom the information is being disclosed; **(c)** The importance of the use or disclosure; **(d)** The likelihood of further disclosure; **(e)** Whether the same result could be achieved with de-identified information; **(f)** The technology available to protect confidentiality of the information; **(g)** The cost to implement administrative, technical and security procedures to protect confidentiality. If we believe that a request from others for disclosure of your entire medical record is unnecessary, we will ask the requestor to document why this is needed, retain that documentation and make it available to you upon request.

**Incidental Disclosure.** We will take reasonable administrative, technical and security safeguards to ensure the privacy of your PHI when we use or disclose it (i.e. we shred all paper containing PHI, require employees to speak with privacy precautions when discussing PHI, we use computer passwords and change them periodically, we use firewall and router protection to the federal standard, we back up our PHI data off-site and encrypted to federal standard, we do not allow unauthorized access to areas where PHI is stored or filed and/or we have any Business Associates sign confidentiality agreements). However, in the event that there is a breach in protecting your PHI, we will follow federal guidelines regarding breaches as prescribed by HIPAA. Breaches will be appropriately documented and reported to the US Dept. of Health and Human Services Office of Civil Rights as well as the Texas Health and Human Services Commission (where applicable). We will also make notification to you and any other parties of significance as required by HIPAA.

**Business Associates.** Business Associates are defined as: an entity, (non-employee) that in the course of their work will directly / indirectly use, transmit, view, transport, hear, interpret process or offer PHI for this Facility. Business Associates and other third parties (if any) that receive your PHI from us will be prohibited from re-disclosing it unless required to do so by law or you give prior express written consent to the re-disclosure. Nothing in our Business Associate agreement will allow our Business Associate to violate this re-disclosure prohibition. Business Associates will sign a strict confidentiality agreement binding them to keep your PHI protected and report any compromise of such information to us, you and the US Dept. of Health and Human Services, as well as other required entities. Our Business Associates required to comply with HIPAA as well as have their subcontractors that may directly or indirectly have contact with your PHI, sign Confidentiality Agreements pursuant to HIPAA as well as comply with HIPAA.

**Super-confidential Information.** If we have PHI about you regarding communicable diseases, disease testing, alcohol or substance abuse diagnosis and treatment, or psychotherapy and mental health records (super-confidential information under the law), we will not disclose it under the General or Healthcare Treatment, Payment and Operations Rules (see above) without your first signing and properly completing our Consent form (i.e. you specifically must initial the type of super-confidential information we are allowed to disclose). If you do not specifically authorize disclosure by initialing the super-confidential information, we will not disclose it unless authorized under the Special Rules (see above) (i.e. we are required by law to disclose it). If we disclose super-

confidential information (either because you have initialed the consent form or the Special Rules authorizing us to do so), we will comply with state and federal law that requires us to warn the recipient in writing that re-disclosure is prohibited.

**Changes to Privacy Policies.** We reserve the right to change our privacy practices (by changing the terms of this Notice) at any time as authorized by law. The changes will be effective immediately upon us making them. They will apply to all PHI we create or receive in the future, as well as to all PHI created or received by us in the past (i.e. to PHI about you that we had before the changes took effect). If we make changes, we will post the changed Notice, along with its effective date, in our office and on our website. Upon request, you will be given a copy of our current Notice.

**Breach Notification.** EHN will notify you of discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

**Authorization.** Absent a purpose otherwise authorized under law, we will not use or disclose your PHI for any purpose or to any person other than as stated in the rules above without your signature (or that of your legal representative) on an authorization for disclosure of PHI which complies with HIPAA. We will not condition your treatment here on whether you sign an authorization for disclosure of PHI (or not).

**Marketing and Fund Raising. Limitations on the disclosure of PHI regarding Remuneration** The disclosure or sale of your PHI without authorization is prohibited. Under HIPAA, this would exclude disclosures for public health purposes, for treatment/payment for healthcare, for the sale, transfer, merger, or consolidation of all or part of this facility and for related due diligence, to any of our Business Associates, in connection with the Business Associate's performance of activities for this facility, to a consumer or beneficiary upon request, and as required by law. In addition, the disclosure of your PHI for research purposes or for any other purpose permitted by HIPAA will not be considered a prohibited disclosure if the only reimbursement received is "a reasonable, cost-based fee" to cover the cost to prepare and transmit your PHI which would be expressly permitted by law. Notably, under HIPAA, an authorization to disclose PHI must state that the disclosure will result in remuneration to the Covered Entity. Notwithstanding the changes in HIPAA, the disclosure of limited data sets (a form of PHI with a number of identifiers removed in accordance with specific HIPAA requirements) for remuneration pursuant to existing agreements is permissible until September 22, 2014, so long as the agreement is not modified within one year before that date.

**Limitation on the Use of PHI for Paid Marketing.** We will, in accordance with federal and Texas law, obtain your written authorization to use or disclose your PHI for marketing purposes, (i.e.: to use your photo in ads) but not for activities that constitute treatment or healthcare operations. To clarify, **Marketing** is defined by HIPAA, as "a communication about a product or service that encourages recipients . . . to purchase or use the product or service." Under HIPAA, we will obtain a written authorization from you prior to recommending you to an alternative therapist, or non-associated Covered Entity.

We will obtain your written authorization prior to using your PHI or making any treatment or healthcare recommendations, should financial remuneration for making the communication be involved from a third party whose product or service we might promote (i.e.: businesses offering this facility incentives to promote their products or services to you). This will also apply to our Business Associate who may receive such remuneration for making a treatment or healthcare recommendations to you. All such recommendations will be limited without your expressed written permission. We must clarify to you that financial remuneration does not include "as in-kind payments" and payments for a purpose to implement a disease management program. Any promotional gifts of nominal value are not subject to the authorization requirement, and we will abide by the set terms of the law to accept or reject these. The only exclusion to this would include: "refill reminders", so long as the remuneration for making such a communication is "reasonably related to our cost" for making such a communication. In accordance with law, this facility and our Business Associates will only ever seek reimbursement from you for permissible costs that include: labor, supplies, and postage. Please note that "generic equivalents", "adherence to take medication as directed" and "self-administered drug or delivery system communications" are all considered to be "refill reminders." Face-to-face marketing communications, such as sharing with you, a written product brochure or pamphlet, is permissible under current HIPAA Law.

**Flexibility on the Use of PHI for Fundraising** HIPAA does not require your authorization should we choose to include you in any fund-raising efforts attempted at this facility. However, we will offer the opportunity for you to "opt out" of receiving future fundraising communications. Simply let us know that you want to "opt out" of such situations. Our commitment to care for and treat you will not be affected by your decision to opt out of fund raising efforts.

**Improvements to Requirements for Authorizations Related to Research** We may seek authorizations from you for the use of your PHI for future research. However, we would have to make clear what those uses are in detail. Also, if we request of you a compound authorization with regards to research, this facility would clarify that when a compound authorization is used, and research-related treatment is conditioned upon your authorization, the compound authorization will differentiate between the conditioned and unconditioned components.

**YOUR RIGHTS REGARDING YOUR PROTECTED HEALTH INFORMATION** If you got this Notice via email or website, you have the right to get, at any time, a paper copy by asking our Privacy Officer. Also, you have the following additional rights regarding PHI we maintain about you:

**To Inspect and Copy** You have the right to see and get a copy of your PHI including, but not limited to, medical and billing records by submitting a written request to our Privacy Officer. Original records will not leave the premises, will be available for inspection only during our regular business hours, and only if our Privacy Officer is present at all times. You may ask us to give you the copies in a format other than photocopies (and we will do so unless we determine that it is impractical) or ask us to prepare a summary in lieu of the copies. We may charge you a fee not to exceed state law to recover our costs (including postage, supplies, and staff time as applicable, but excluding staff time for search and retrieval) to duplicate or summarize your PHI. We will not condition release of the copies on summary of payment of your outstanding balance for professional services if you have one). We will comply with federal law to provide your PHI in an electronic format, when you provide us with proper written request. Paper copies will also be made available. We will respond to requests in a timely manner, without delay for legal review, or, in less than thirty days if submitted in writing, and in ten business days or less if malpractice litigation or pre-suit production is involved. We may deny your request in certain limited circumstances. You may be denied access to your records, if in our opinion: (1) release of such information would be harmful to you; (2) you, acting in the capacity of legal representative of a minor or incapacitated individual and requesting records regarding that minor or incapacitated individual, we deem that release of such information to you would be harmful to the minor or incapacitated individual where such minor or incapacitated individual is suspected of being abused by you, or (3) any other permissible reason as allowed under federal or state law. If we deny your request, you may ask for a review of that decision. If required by law, we will select a licensed health-care professional (other than the person who denied your request initially) to review the denial and we will follow his or her decision. If we select a licensed healthcare professional who is not affiliated with us, we will ensure a Business Associate Agreement is executed that prevents re-disclosure of your PHI without your consent by that outside professional.

**To Request Amendment / Correction** If another doctor involved in your care tells us in writing to change your PHI, we will do so as expeditiously as possible upon receipt of the changes and will send you written confirmation that we have made the changes. If you think PHI we have about you is incorrect, or that something important is missing from your records, you may ask us to amend or correct it (so long as we have it) by submitting a “**Request for Amendment / Correction**” form to our Privacy Officer. We will act on your request within 30 days from receipt, but we may extend our response time (within the 30-day period) no more than once and by no more than 30 days, or as per federal law allowances, in which case we will notify you in writing why and when we will be able to respond. If we grant your request, we will let you know within five business days, make the changes by noting (not deleting) what is incorrect or incomplete and adding to it the changed language, and send the changes within five business days to persons you ask us to and persons we know may rely on incorrect or incomplete PHI to your detriment (or already have). We may deny your request under certain circumstances (i.e. it is not in writing, it does not give a reason why you want the change, we did not create the PHI you want changed (and the entity that did can be contacted), it was compiled for use in litigation, or we determine it is accurate and complete). If we deny your request, we will (in writing within five business days) tell you why and how to file a complaint with us if you disagree, that you may submit a written disagreement with our denial (and we may submit a written rebuttal and give you a copy of it), that you may ask us to disclose your initial request and our denial when we make future disclosure of PHI pertaining to your request, and that you may complain to us and the US Dept. of Health and Human Services.

**Faxing** When you request us to fax your PHI as an alternative communication, we may agree to do so, but only after having our Privacy Officer or treating doctor review that request. For this communication, our Privacy Officer will confirm that the fax number is correct before sending the message and ensure that the intended recipient has sole access to the fax machine or computer before sending the message; confirm receipt, locate our fax machine or computer in a secure location so unauthorized access and viewing is prevented; use a fax cover sheet so the PHI is not the first page to print out (because unauthorized persons may view the top page); and attach an appropriate notice to the message.

**Practice Transition** If we sell or otherwise transfer our practice, our consumer records (including but not limited to your PHI) may be disclosed and physical custody may be transferred to the purchasing/transferring healthcare provider, but only in accordance with the law. The healthcare provider who is the new records owner will be solely responsible for ensuring privacy of your PHI after the transfer and you agree that we will have no responsibility for (or duty associated with) transferred records. If ever applicable to EHN (as EHN is a governmental entity not owned by any entity or individual), if all the owners of our practice die, our consumer records (including but not limited to your PHI) must be transferred to another healthcare provider within 90 days to comply with state and federal laws. Before we transfer records in either of these two situations, our Privacy Officer will obtain a Business Associate Agreement from the purchaser and review your PHI for super-confidential information (i.e. communicable disease records), which will not be transferred without your express written authorization (indicated by your initials on our consent form).

**Collections** If we use or disclose your PHI for collections purposes, we will do so only in accordance with the law.

**To Request an Accounting of Disclosures** You may ask us for a list of those who got your PHI from us by submitting a “**Request for Accounting of Disclosures**” form to us. The list will not cover some disclosures (i.e. PHI given to you, given to your legal representative, given to others for treatment, payment or health-care-operations purposes). Your request must state in what form you want the list (i.e. paper or electronically) and the time period you want us to cover, which may be up to but not more than the last six years (excluding dates before April 14, 2003). If you ask us for this list more than once in a 12-month period, we may charge you a reasonable, cost-based fee to respond, in which case we will tell you the cost before we incur it and let you choose if you want to withdraw or modify your request to avoid the cost.

**To Request Restrictions** You may ask us to limit how your PHI is used and disclosed (i.e. in addition to our rules as set forth in this Notice) by submitting a written “**Request for Restrictions on Use, Disclosure**” form to us (i.e. you may not want us to disclose your surgery to family members or friends involved in paying for our services or providing your home care). If we agree to these additional limitations, we will follow them except in an emergency where we will not have time to check for limitations. Also, in some circumstances we may be unable to grant your request (i.e. we are required by law to use or disclose your PHI in a manner that you want restricted, you signed an authorization form, which you may revoke, that allows us to use or disclose your PHI in the manner you want restricted; in an emergency).

**To Request Alternative Communications** You may ask us to communicate with you in a different way or at a different place by submitting a written “**Request for Alternative Communication**” Form to us. We will not ask you why and we will accommodate all reasonable requests (which may include: to send appointment reminders in closed envelopes rather than by postcards, to send your PHI to a post office box instead of your home address, to communicate with you at a telephone number other than your home number). You must tell us the alternative means or location you want us to use and explain to our satisfaction how payment to us will be made if we communicate with you as you request.

**Records of Minors** Where applicable, and in compliance with state law, including, but not limited to Texas Family Code Chapter 32, a parent or guardian may not have access to the all of the records regarding their minor child and some information disclosed to EHN by the minor child may be withheld from the parent or guardian.

**Confidentiality of Alcohol and Drug Abuse Consumer Records** To the extent applicable to your specific treatment, the confidentiality of alcohol and drug abuse consumer records maintained by EHN is protected by federal law and regulations. Generally, EHN may not say to a person outside the program that a consumer attends a substance abuse treatment program, or disclose any information identifying a consumer as an alcohol or drug abuser Unless: (1) The consumer consents in writing; (2) The disclosure is allowed by a court order; or (3) The disclosure is made to medical personnel in a medical emergency or to qualified personnel for research, audit, or program evaluation. Violation of the federal law and regulations by a program is a crime. Suspected violations may be reported to appropriate authorities in accordance with federal regulations. Federal law and regulations do not protect any information about a crime committed by a consumer either at EHN or against any person who works for EHN or about any threat to commit such a crime. Federal laws and regulations do not protect any information about suspected child abuse or neglect from being reported under Texas law to appropriate authorities.

**COMPLAINT PROCESS:** If you want more information or if you believe that EHN has violated your privacy rights (i.e. you disagree with a decision of ours about inspection/ copying, amendment/ correction, accounting of disclosures,

restrictions or alternative communications), we want to make it right. We never will penalize you for filing a complaint. To do so, please file a formal, written complaint with:

- **EHN:** Orlando Gonzalez, Privacy Officer, P.O. Box 9997, El Paso, Texas 79990; (915) 887-3410; [ogonzalez@ehnel Paso.org](mailto:ogonzalez@ehnel Paso.org);
- **Health and Human Services Consumer Services and Rights Protection/Ombudsman Office:** (512) 206-5670 or (800) 252-8154 (toll free) P.O. Box 12668, Austin, Texas 78711;
- **U.S. Dept. of Health and Human Services** 200 Independence Avenue, S.W., Washington, D.C. 20201 (800) 368-1019 (toll free).

**You must file your complaint within 180 days of when you knew or should have known about the event that you think violated your privacy rights.**

You may also contact: **Office of Attorney General**; P.O. Box 12548, Austin, Texas 78711; (800) 463-2100 (toll free); [www.oag.state.tx.us](http://www.oag.state.tx.us)

For complaints against alcohol/drug abuse treatment programs, contact the US Attorney's Office for the judicial district in which the violation occurred. To locate this office, consult the telephone book blue pages.

**EHN WILL NOT RETALIATE AGAINST  
YOU IF YOU FILE A COMPLAINT.**

The effective date of this NPP is August 1, 2016 and replaces any previous notices of privacy practices issued by EHN, El Paso MHMR or any successor entity. These privacy practices are in accordance with the original HIPAA enforcement effective April 14, 2003 and updated to Omnibus Rule effective March 26, 2013 and will remain in effect until we replace them as specified by federal and/or Texas law. You have rights under HIPAA and other laws; this NPP advises you of those rights. You may have other rights under other federal and state laws which may or may not be stated herein, however the failure of EHN to not specifically refer to such laws does not necessarily impact your rights under those laws.



Client #:

Medicaid #:

Unit:

### Consent to Release Information

1. The person whose information may be used, disclosed, or exchanged is:

Client Name:

2. I authorize the designated staff at Emergence Health Network to Disclose, Use, or Receive my protected health information: (select only ONE of the following)

Disclose       Use       Receive

3. Information to be disclosed to/exchanged with:

Name:    
City:  State:  Zip:   
Phone:  Fax:

4. Information to be released/received/used:

Covering the period(s) of treatment: From:  To:

Progress Notes: (make a selection below)  
     Medical Progress Notes       Psychiatric Evaluation       Labs  
     Caseworker Progress Notes       Discharge Documentation       Billing Records  
     Therapy Progress Notes  
 Other (specify below)

Mail Copies (complete address):

Pick-Up copies (location of pick-up):

Fax copies (attention to):

5. I also authorize the disclosure or receipt of my health information regarding (a selection is required to consent or deny the release of the following information):

Yes  No    Alcohol or Substance Abuse Records  
 Yes  No    HIV/AIDS Records  
 Yes  No    Genetic Information (including Genetic Test Results)

6. Purpose of Receipt/Disclosure:

- at my request                       legal purposes                       billing and claims
- educational purposes               treatment/continuity of care       to verbally disclose the care and treatment I receive

other:

7. The persons or organizations receiving any Disclosure of this information will be prohibited by law from re-disclosing any information received based upon this consent and will be notified of that fact in every disclosure.

Consent:

Effective Date:  Expiration Date:

I understand that this permission may be revoked. I also understand that records disclosed before this permission is revoked may not be retrieved. Any person or organization that relied on this permission may continue to use or disclose records and protected health information as needed to complete work that began because this permission was given.

I DENY CONSENT (Revoke)

I understand that EHN is sensitive about client’s trauma and realizes the effects it can have. EHN encourages clients to participate in treatment decision making by giving them a voice and choice about the information that is shared with EHN and its staff. EHN promotes a trauma informed approach to its care and interactions with patients to reduce re-traumatization.

I am the person or personal representative of the person whose records will be used, disclosed, or exchanged. I give permission to use, disclose, and exchange records as described in this document.

I understand that Emergence Health Network (EHN) may share my health information in EHN's files with another medical provider to help with my treatment with that other provider with or without my permission as allowed under federal and state privacy laws (45 CFR 164.506(c)(4), Tex. Health and Safety Code 611.004(a)(7), Tex. Health and Safety Code 81.103(b)(5)).

I understand that I do not have to give consent to share alcohol and/or substance abuse treatment information with my medical provider(s), but by authorizing disclosure on page one (1) of this form, I freely choose to do so. I also understand that I may revoke, at any time, my authorization for the medical provider(s) to have access to alcohol and/or substance abuse treatment information, however, other information regarding my treatment with EHN may be shared with the medical provider(s) as allowed under HIPAA and any other federal or state privacy laws. My decision to revoke this authorization shall only apply to information which has not already been shared with the medical provider(s).

If there is any information in my medical record regarding current or past alcohol and/or substance abuse treatment, federal law prohibits EHN from sharing that information without my permission, unless in certain situations such as a medical emergency (42 CFR Part 2). The sharing of this information may be helpful to my medical provider(s) for my treatment.

I understand that my permission to share this information does not automatically mean that I have an alcohol or substance abuse problem, or that I have ever used or abused alcohol or drugs. Even though I may not have information in my medical record related to alcohol and/or substance abuse treatment, my permission to share this information will allow EHN to share my medical records quicker to my medical provider(s).

If I choose not to give permission to share alcohol and/or substance abuse treatment information, EHN will still provide my information to my medical provider(s), however, every document in my medical record will have to be reviewed to ensure that the substance and/or substance abuse treatment information is not shared.

I understand that the review of my medical record may require several hours and that an immediate turn-around cannot be guaranteed.

Please allow 10 business days for your request

<b>Client Signature:</b>		<b>Date:</b>	
--------------------------	--	--------------	--

<b>Parent/Guardian Signature:</b> <i>(if not applicable, enter "N/A")</i>		<b>Date:</b>	
<b>LAR Signature:</b> <i>(if not applicable, enter "N/A")</i>		<b>Date:</b>	
<b>Staff Name:</b>		<b>Title:</b>	

<b>For Office Use ONLY:</b> <input type="checkbox"/> Process Request (allow 10 business days) <input type="checkbox"/> Upload into client's chart ONLY
---

**Confidential Communication Request Form**

**EMERGENCY HEALTH NETWORK**

**CONFIDENTIAL COMMUNICATION REQUEST FORM**

Name:

Other Names:

Address:

Phone:

DOB:

You or your Personal Representative (PR)/Legal Authorized Representative (LAR) have the right to request that you received communications from Emergence Health Network (EHN) at an alternative location or by alternative means.

- If you or your PR wants an alternative location or means of communication to be used by EHN, you must specify such alternative location or means of communication in this request.
- You will be notified of EHN's response to your request in writing.
- Even if EHN agrees to your request, there may be times when EHN needs to contact you at any known address and/or by any available means.
- Even if EHN agrees to your request, this decision may be revoked by EHN if the alternative location or means of communication become unreasonable. Written notice of the revocation will be provided to you or your PR. The revocation will be effective only after such notice is given.

I am asking EHN to communicate with me in the following manner (specify location or manner of communication):

Declined

Mail

Phone

Email

\_\_\_\_\_  
Your signature or Personal Representative's signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Print Name of signer

THE FOLLOWING INFORMATION IS NEEDED IF SIGNED BY PERSONAL REPRESENTATIVE:

Type of authority (e.g., court appointed, custodial parent): \_\_\_\_\_

**For EHN Use**

Approved:

Denied:

**42 CFR Part 2- Requisite Language****42 CFR § 2.31 Consent requirements. (2017)**

(a) Required elements for written consent. A written consent to a disclosure under the regulations in this part may be paper or electronic and must include:

- (1) The name of the patient.
- (2) The specific name(s) or general designation(s) of the part 2 program(s), entity(ies), or individual(s) permitted to make the disclosure.
- (3) How much and what kind of information is to be disclosed, including an explicit description of the substance use disorder information that may be disclosed.
- (4)

- (i) The name(s) of the individual(s) to whom a disclosure is to be made; or
- (ii) Entities with a treating provider relationship with the patient. If the recipient entity has a treating provider relationship with the patient whose information is being disclosed, such as a hospital, a health care clinic, or a private practice, the name of that entity; or
- (iii) Entities without a treating provider relationship with the patient.

(A) If the recipient entity does not have a treating provider relationship with the patient whose information is being disclosed and is a third-party payer, the name of the entity; or

(B) If the recipient entity does not have a treating provider relationship with the patient whose information is being disclosed and is not covered by paragraph (a)(4)(iii)(A) of this section, such as an entity that facilitates the exchange of health information or a research institution, the name(s) of the entity(-ies); and

- (1) The name(s) of an individual participant(s); or
- (2) The name(s) of an entity participant(s) that has a treating provider relationship with the patient whose information is being disclosed; or
- (3) A general designation of an individual or entity participant(s) or class of participants that must be limited to a participant(s) who has a treating provider relationship with the patient whose information is being disclosed.

(i) When using a general designation, a statement must be included on the consent form that the patient (or other individual authorized to sign in lieu of the patient), confirms their understanding that, upon their request and consistent with this part, they must be provided a list of entities to which their information has been disclosed pursuant to the general designation (see § 2.13(d)).

(ii) [Reserved]

(5) The purpose of the disclosure. In accordance with § 2.13(a), the disclosure must be limited to that information which is necessary to carry out the stated purpose.

(6) A statement that the consent is subject to revocation at any time except to the extent that the part 2 program or other lawful holder of patient identifying information that is permitted to make the disclosure has already acted in reliance on it. Acting in reliance includes the provision of treatment services in reliance on a valid consent to disclose information to a third-party payer

(7) The date, event, or condition upon which the consent will expire if not revoked before. This date, event, or condition must ensure that the consent will last no longer than reasonably necessary to serve the purpose for which it is provided.

(8) The signature of the patient and, when required for a patient who is a minor, the signature of an individual authorized to give consent under § 2.14; or, when required for a patient who is incompetent or deceased, the signature of an individual authorized to sign under § 2.15. Electronic signatures are permitted to the extent that they are not prohibited by any applicable law.

(9) The date on which the consent is signed.

(b) Expired, deficient, or false consent. A disclosure may not be made on the basis of a consent which:

- (1) Has expired;
- (2) On its face substantially fails to conform to any of the requirements set forth in paragraph (a) of this section;
- (3) Is known to have been revoked; or
- (4) Is known, or through reasonable diligence could be known, by the individual or entity holding the records to be materially false.

**42 CFR § 2.32 Prohibition on re-disclosure. (2017)**

(a) Notice to accompany disclosure. Each disclosure made with the patient's written consent must be accompanied by the following written statement: This information has been disclosed to you from records protected by federal confidentiality rules (42 CFR part 2). The federal rules prohibit you from making any further disclosure of information in

this record that identifies a patient as having or having had a substance use disorder either directly, by reference to publicly available information, or through verification of such identification by another person unless further disclosure is expressly permitted by the written consent of the individual whose information is being disclosed or as otherwise permitted by 42 CFR part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose (see § 2.31). The federal rules restrict any use of the information to investigate or prosecute with regard to a crime any patient with a substance use disorder, except as provided at §§ 2.12(c)(5) and 2.65.

(b) [Reserved]

## Texas Family Code Section 32.004

### Texas Family Code Sec. 32.004. Consent to Counseling. (2017)

(a) A child may consent to counseling for:

- (1) suicide prevention;
- (2) chemical addiction or dependency; or
- (3) sexual, physical, or emotional abuse.

(b) A licensed or certified physician, psychologist, counselor, or social worker having reasonable grounds to believe that a child has been sexually, physically, or emotionally abused, is contemplating suicide, or is suffering from a chemical or drug addiction or dependency may:

- (1) counsel the child without the consent of the child's parents or, if applicable, managing conservator or guardian;
- (2) with or without the consent of the child who is a client, advise the child's parents or, if applicable, managing conservator or guardian of the treatment given to or needed by the child; and
- (3) rely on the written statement of the child containing the grounds on which the child has capacity to consent to the child's own treatment under this section.

(c) Unless consent is obtained as otherwise allowed by law, a physician, psychologist, counselor, or social worker may not counsel a child if consent is prohibited by a court order.

(d) A physician, psychologist, counselor, or social worker counseling a child under this section is not liable for damages except for damages resulting from the person's negligence or willful misconduct.

(e) A parent, or, if applicable, managing conservator or guardian, who has not consented to counseling treatment of the child is not obligated to compensate a physician, psychologist, counselor, or social worker for counseling services rendered under this section.

## Research Request Application

This application is to request permission from Emergence Health Network to use data on EHN systems, paper records, or verbal interviews for the purpose of research projects as part of an internship for licensure, higher education, certification training, and other purposes. A panel from different areas of expertise will review this application for approval. Areas that will be considered for approval are consumer privacy, treatment interference; and operations impact. After review of the application by all areas you will receive written notification of your request.

Requestor Name/Title:		Date:	
Employment Status:	Full-Time	Part-Time	Intern Volunteer
Assigned Program/Unit:		Supervisor Name:	

Purpose (Describe the research in detail include audiences, intended use of data, final report summaries):

Type of Data (demographic, diagnosis, outcomes):	
Alcohol/Drug Abuse Data (diagnosis, medications, assessments):	
Time frames to be reviewed (begin and end):	
# Of Clients to be reviewed:	
Format of data (report or chart reviews, de-identified, patient identifiers):	
Format of final report produced:	
Client Consent/Authorization (will clients be notified of their data use for research):	

School or Entity:			
Institutional Review Board Approval:		Remuneration: If yes, Name Individual or Entity	
Will data be published If yes, When and Who:			

List Documents/Attach (approvals, consents, project information):

Internal Use Only
-------------------

Administrative Director of Health Information/Privacy Officer		
Comments:		
Approved	Deny	Other

Legal		
Comments:		
Approved	Deny	Other

Chief Nursing Officer		
Comments:		
Approved	Deny	Other

Chief Medical Officer		
Comments:		
Approved	Deny	Other

Associate Chief Executive Officer		
Comments:		
Approved	Deny	Other

Chief Executive Officer		
Comments:		
Approved	Deny	Other

# Appendix B— Breach Reporting

## PRIVACY BREACH ASSESSMENT

1) Was Private Information Involved?  Yes  No

2) Was the Private Information encrypted?  Yes  No

3) Description of breach:

a) What data elements have been breached? Health information, social insurance numbers and financial information that could be used for identity theft are examples of sensitive personal information.

b) What possible use is there for the private information? For instance, can the information be used for fraudulent or otherwise harmful purposes?

c) What was the date that the breach was discovered? \_\_\_\_\_

d) What is believed to be the date that the breach occurred? \_\_\_\_\_

2) Cause and Extent of the Breach

a) What is the cause of the breach?

b) Is there a risk of ongoing or further exposure of the information?  Yes  No

c) What was the extent of the unauthorized collection, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, including in mass media or online?

d) Is the information encrypted or otherwise not readily accessible?  Yes  No

e) What steps have already been taken to minimize the harm?

3) Individuals Affected by the Breach

a) How many individuals are affected by the breach?

1. Who was affected by the breach:

Employees

Customer-owners

Volunteers

Contractors

Service providers

Other individuals/organizations

4) Foreseeable Harm from the Breach

a) Is there any relationship between the unauthorized recipients and the data subject?

Yes  No

b) Is any of the information or the individual whose information was compromised subject to additional protections, such as court orders, temporary restraining orders, protections from harm, etc.?

2. What harm to the individuals will result from the breach? Harm that may occur includes:

Security risk (e.g., physical safety)

Identity theft or fraud

Loss of business or employment opportunities

Hurt, humiliation, damage to reputation or relationships

Other (please specify):

d) What harm could result to the organization as a result of the breach?

Loss of trust in the organization

Loss of assets

Financial exposure

Other (please specify):

e) What harm could result to the public as a result of the breach?

- Risk to public health
- Risk to public safety
- Other (please specify):

1. Privacy Act Analysis

- a. Determine whether the breached information was in the control and possession of a Federal agency. If not, the Privacy Act does not apply, and the analysis below is not necessary.
- b. Determine if the incident poses a risk to individuals. The following factors shall be considered when assessing the likely risk of harm and level of impact for a potential or confirmed privacy breach:
  - i. Nature of the data elements breached in light of their context and the broad range of potential harms that may result from their disclosure to unauthorized individuals;
  - ii. Potential harm to reputation of individuals;
  - iii. Potential for harassment or prejudice;
  - iv. Potential for identity theft, including any evidence that breached information is actually being used;
  - v. Number of individuals affected;
  - vi. Likelihood that breach was the result of a criminal act or will result in criminal activity;
  - vii. Likelihood the information is accessible and usable by unauthorized individuals;
  - viii. Likelihood the breach may lead to harm; and
  - ix. Ability to mitigate the risk of harm.
- c. If an identity theft risk is present, tailor the response to the nature and scope of the risk presented. Notice may not be required in all circumstances, so the response team should assess the situation and determine if notification to individuals is necessary. In some cases, notification may actually increase a risk of harm, in which case Emergence Health Network should delay notification until proper safeguards can be instituted. The analysis of whether notification is necessary should be based on the following factors:
  - i. Number of individuals affected;
  - ii. Urgency with which individuals need to receive notice;
  - iii. Whether other public and private sector agencies need notification, particularly those that may be affected or may play a role in mitigating the breach;
  - iv. Contact information available for affected individuals (first-class mail shall be the primary means for providing notification, but telephone or email may be appropriate when there is an urgent need); and
  - v. Whether media outlets may be the best way to alert affected individuals and mitigate any risk.
- d. Written notification should include the following elements:
  - i. Brief description of what happened, including the date of the breach and its discovery;
  - ii. Description of the types of information involved in the breach;
  - iii. Statement whether the information was protected, if such information would be beneficial and would not compromise security;
  - iv. Steps individuals should take to protect themselves from harm;
  - v. What Emergence Health Network is doing to investigate and mitigate the breach; and
  - vi. Who affected individuals should contact for more information, including a toll-free telephone number, e-mail address and postal address.
- e. If the CEO determines that public notification through the media is necessary, it should also post notification of the breach on its website, with the same information required for written notification to the individual. The posting should provide answers to frequently asked questions and other talking points.

2. State Data Breach Analysis

- a. Identify the state of residence of all individuals affected by the breach.

- b. Consult individual state data breach statutes to determine if a state's particular data breach statute is applicable to Emergence Health Network.
- c. Consult individual state data breach statutes to determine if a breach has occurred under a state's particular data breach statute.
- d. Consult individual state data breach statutes to determine breach notification steps to take in accordance with a state's particular data breach statute.

### 3. HIPAA/HITECH Analysis

- a. Determine whether the breached information was Protected Health Information (individually identifiable health information as defined by HIPAA). If not, HIPAA/HITECH breach reporting requirements do not apply, and the analysis below is not necessary.
- b. If breached information was PHI, determine whether the PHI was secured or unsecured. Unsecured PHI is defined as PHI that is not secured through a means that HHS has approved as rendering the PHI unusable or unreadable to unauthorized persons. If PHI was secured, no reporting is necessary under HIPAA and you can proceed to Step 2.
- c. If PHI was unsecured, it constitutes an official breach under HIPAA if it "compromises the security or privacy of the PHI" and does not meet one of the exceptions to breach.
  - i. Compromises the security or privacy – this means that it poses a significant risk of financial, reputational or other harm to the individual. Sections 2 and 4 of the Privacy Breach Questionnaire should assist with this analysis. Key factors to consider:
    - 1. To whom was the information disclosed?
    - 2. What type of information was breached?
    - 3. How easily can the information be redistributed?
  - ii. Exceptions to breach (these factors are fairly subjective and any analysis resulting in the conclusion that a disclosure meets one of these exceptions should be documented and retained for six years):
    - 1. Good faith and unintentional acquisition, access or use by a person working under the authority of a covered entity or business associate, which is within the scope of authority and does not result in further use or disclosure.
    - 2. Disclosures between persons at the same covered entity, business associate or organized health care arrangement if persons are authorized and information will not be further used or disclosed.
    - 3. Disclosure where the covered entity or business associate has the good faith belief that the information could not have been retained (for example, a person drops their jump drive overboard on a moving cruise ship).
- d. If the disclosure is found to meet one of these exceptions or is not found to compromise the security or privacy of the PHI, proceed to Step 2. If the disclosure does not meet one of the exceptions to breach, and it is found to compromise the security or privacy of the PHI, the next step is to determine how to mitigate the breach and protect the individual. Part of the mitigation and protection efforts would include notification, but they may also include instituting additional security measures, changing a person's account number, notifying police of the breach and other appropriate measures.
- e. After determining and instituting mitigation and protection efforts, Emergence Health Network must fulfill its obligations to notify the affected individuals of the breach. Notice must be provided within 60 days of discovery<sup>1</sup>, unless authorized to delay by law enforcement Associates. First, Emergence Health Network should determine how notice should be sent to the individual. The following rules apply:
  - i. If contact information is sufficient and no more than 500 residents in the state are affected, written notification should be sent by first class mail.
  - ii. If contact information is not sufficient for more than 10 individuals, notification must also be on the Emergence Health Network home page and in major media (print or broadcast).
  - iii. If more than 500 residents are affected, notification must also be made to major media, even if contact information is sufficient for all affected persons.
- f. Notice should be carefully drafted to include the following required information, without any unnecessary information that may result in additional questions or concerns from affected individuals:

---

<sup>1</sup> Discovery is defined as when the breach is known or should reasonably have been known.

- i. Brief description of the breach, including the date of the breach and date of discovery.
    - ii. Description of the types of PHI involved.
    - iii. Steps the individual should take to protect themselves.
    - iv. Brief description of steps Emergence Health Network is taking to mitigate, investigate and protect.
    - v. Contact procedures for questions or additional information, including a toll-free telephone number, email, Web site or address.
  - g. If more than 500 persons are affected, notice must also be provided to the U.S. Department of Health and Human Services. If 500 or less are affected, the notice should be kept in an annual log of breaches.
4. Breach Analysis Follow-Up: Once the breach analysis is complete and notice is provided, Emergence Health Network should review policies, procedures and security measures to incorporate any necessary updates or changes.

## Sample Breach Notification Letter

### **POSSIBLE UNAUTHORIZED DISCLOSURE OF PROTECTED HEALTH INFORMATION**

Dear Mr./Mrs.,

We are sending you this letter to let you know that your protected health information may have been shared or seen without approval from you or Emergence Health Network (EHN). EHN is the local mental health authority for El Paso County and has previously been known as El Paso MHMR and Life Management Center. This letter is to let you know EHN is taking steps to correct the situation that caused your information to be exposed and to protect your information in the future.

**What happened:** On MONTH XX, 201X a (BREIF DESCRIPTION OF INCIDENT, WHO WAS INVOLVED, TYPE OF PHI DISCLOSED) The XXXXXXXXXXXXX contained your first and last name, address, phone number, and case number.

**What EHN is doing:** The supervisor of clinic notified the privacy officer to investigate the incident and determine if a breach had occurred. The Department of State and Health Services has been notified of the breach and we are taking steps to keep this from happening again by using more secure methods for transporting, maintaining, and safeguarding your protected health information. We have not received any indication that the information has been accessed or used by an unauthorized individual.

**What you can do now:** At this time, we don't have any proof that your personal information was misused. However, EHN suggests that you can take the following steps to protect your personal information:

1. Call one of the credit reporting agencies listed below. Ask for a fraud alert to be put on your credit report. A fraud alert will not let anyone open credit accounts in your name for a period of time.
2. Ask for a copy of your credit report from all three credit reporting agencies. (If you haven't gotten credit reports in the last year, you can get them free by going to [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com) or by calling 1-877-322-8228.)
3. Carefully check your: (a) account statements, (b) benefit notices, (c) medical records, and (d) credit reports.

#### **Credit agencies:**

**Equifax** - [www.equifax.com](http://www.equifax.com)  
PO Box 740256 - Atlanta, GA  
30374  
Fraud hotline: 1-800-685-1111  
(toll-free)

**Experian** - [www.experian.com](http://www.experian.com)  
PO Box 2002 - Allen, TX 75013  
Fraud hotline: 1-888-397-3742  
(toll-free)

**TransUnion LLC** - <https://fraud.transunion.com>  
PO Box 2000 - Chester, PA 19022-2000  
Fraud hotline: 1-800-680-7289 (toll-free)

**What you should do if you think your personal information is being misused:** If you think your personal information is being misused, file a report with your local police, sheriff, or both. Make sure to get a copy of the report. Give a copy to your banks, credit card companies, and the credit agencies. You can learn more about the misuse of personal facts and identity theft from:

**Attorney General of Texas**

Identity theft: [www.texasfightsidtheft.gov](http://www.texasfightsidtheft.gov)

Health privacy laws:

[www.oag.state.tx.us/consumer/hipaa.shtml](http://www.oag.state.tx.us/consumer/hipaa.shtml)

Consumer Protection Hotline: 1-800-621-0508 (toll-free)

**Federal Trade Commission**

Identity theft: [www.ftc.gov/bcp/edu/microsites/idtheft](http://www.ftc.gov/bcp/edu/microsites/idtheft)

Identity Theft Helpline: 1-877-438-4338 (toll-free)

**If you have questions:** Call Emergence Health Network's Privacy Officer, Orlando Gonzalez. **Phone:** 1-844-637-6466

**Email:** [yourprivacy@ehnpaso.org](mailto:yourprivacy@ehnpaso.org)

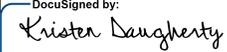
We are sorry for any inconvenience this incident may have caused you.

## Reporting A Possible Breach

### *Reporting a Possible Breach*

1. Any employee who becomes aware of a possible breach of privacy involving Private Information in the custody or control of EHN will immediately inform their supervisor/manager.
2. Supervisor/manager notifies EHN's Privacy Officer (PO) by phone or email alerting PO of the situation.
3. PO will instruct supervisor/manager, in consultation with employee reporting the possible breach, to complete an incident report via the Ethics Point reporting system (or its successor). To make a report, one of two options is available:
  - a. Dial toll-free at 1-844-252-3072
  - b. Electronic submission at <http://ehn.ethicspoint.com> can be accessed from any computer and by smart phone technology
    - i. Click on upper right "MAKE A REPORT"
    - ii. Then click on "CONFIDENTIALITY"
    - iii. Under CONFIDENTIALITY, two additional options and their respective definitions is provided to help inform the incident report:
      1. Option 1: Disclosure of Confidential Information
      2. Option 2: Health Insurance Portability and Accountability Act.
    - iv. Upon selecting one of the aforementioned options, answer every question on the reporting template providing sufficient detail as possible.
    - v. Notification to PO and Ethics Point should occur immediately upon discovery of a possible breach or before the end of your shift if other duties interfere, however, in no case should notification occur later than twenty-four (24) hours after discovery.
  - c. The supervisor/manager will verify the circumstances of the possible breach and inform the Privacy Officer and the division Chief within twenty-four (24) hours of the initial report.
4. You may call the Privacy Officer directly at 915-493-1596.
  - a. Provide the Privacy Officer with as much detail as possible.
  - b. Be responsive to requests for additional information from the Privacy Officer.
  - c. Be aware that the Privacy Officer has an obligation to follow up on any reasonable belief that Private Information has been compromised.
5. The Privacy Officer will notify the CIO, CCO and EHN's Legal Counsel and will react, as appropriate, by taking into consideration the seriousness and scope of the breach.

### POLICY APPROVALS:

CEO Approval:	<small>DocuSigned by:</small>  <small>C167C8463EE94B5...</small>	Date:	10/16/2020   12:13 PM PDT
---------------	---	-------	---------------------------

## Privacy Policy Updates

Date: 5/21/20

The Administrative Director of Health Information, Orlando Gonzalez, has made the following changes to the Privacy Policy and is requesting a review. Below is a summary of the sections that were updated or added in the Privacy Policy (changes are marked in red).

Location of Changes & Brief Description	Updates or Additions
<p><b>Title Page, Page 1-</b></p> <p>Date and the version of the Privacy Policy were updated</p>	<p>Last Revision Date</p> <p>5/26/20</p> <p>Version 4</p>
<p><b>Introduction Page, Page 4-</b> Certified Community Behavioral Health Clinics (CCBC) and Trauma Informed Care Time for Organizational Change (TIC TOC) Program requirements were incorporated into the Privacy Policy. Language supporting these initiatives was adopted.</p>	<p>Purpose</p> <p>This policy defines controls to safeguard the protected health information of Emergence Health Network consumers. Ensure the integrity and compliance of federal and state regulations as it pertains to protected health information. It serves as a central policy document with which all employees and contractors must be familiar; and defines actions and prohibitions that all users must follow. The policy provides Emergence Health Network with policies and guidelines concerning the access, disclosure, use, breach notification, investigations, and audits of protected health information.</p> <p>Ensuring that communication between EHN associates, consumers, and consumer families occurs timely and is the least restrictive to effective treatment. Effective treatment of consumers is achieved by eliminating re-traumatizing practices that are often used in many service systems. EHN has incorporated a trauma-informed culture by making change to its policies and procedures; staff trainings; and interventions. This trauma informed culture gives the client shared decision making, choice, and goal setting of their treatment.</p>
<p><b>Definitions, Page 10-</b> Added telecommuting to the definitions.</p>	<p>Telecommuting</p> <p>Telecommuting, also called telework, teleworking, working from home, mobile work, remote work, and flexible workplace is a work arrangement in which employees do not commute or travel to a central place of work, such as an office building, warehouse, or store. Teleworkers often use mobile telecommunications technology such as a Wi-Fi-equipped laptop or tablet computers and smartphones to work.</p>
<p><b>Safeguarding Confidential Information Off-site, Page 24-</b> Additional items involving the safeguarding of protected health information when</p>	<p>1.10.2 Safeguarding Confidential Information Off-site</p> <p>All the safeguard requirements for the worksite apply equally to any use of confidential information away from or off-site from the workplace. Files and records should be securely transported.</p> <p>Computer/Electronic Format</p> <ul style="list-style-type: none"> <li>Associates authorized to use any EHN owned computing device (e.g.,</li> </ul>

<p>working off-site or out of the office were added. Safeguarding of protected health information on paper was added.</p>	<p><b>laptop, desktop, tablet, smartphone, etc.)</b> off-site are responsible for assuring the security, as well as minimize the risk of loss of the device and its contents.</p> <ul style="list-style-type: none"> <li>• <b>On a case by case basis or under unusual circumstances associates may be given authorization to conduct official EHN business using personal computers for a limited amount of time.</b> Associates should observe security protocols to prevent unauthorized users from accessing confidential information. <b>Lock computer screen when stepping away from the computer when at home or a client's home.</b> Shared use of computers with family member or others who are not part of the work force create a risk of inadvertent disclosure of confidential information.</li> <li>• <b>Transferring data to personal devices such as computers, tablets, or cell phones is prohibited. Protected health information should not be sent to personal emails or stored in the cloud or thumb drives. Protected health information should not be sent to or from family members devices or accounts.</b></li> <li>• Associates are responsible for securing digital camera images. Digital cameras can store confidential information that can be accessed by anyone who has the camera.</li> <li>• <b>Protected health information should not be posted on any social media platforms.</b></li> </ul> <p>Telephone</p> <ul style="list-style-type: none"> <li>• Associates should ensure care when using company issued telephones outside of the worksite. Cell phones, smart phones or other telephones require care to protect confidential information.</li> <li>• Associates should avoid using identifiable information about clients unless associates have taken reasonable efforts to assure the privacy of the call.</li> <li>• Transmitting identifiable information about clients is not permitted from <b>or to</b> personal telephones. This can include up to text messaging, <b>descriptions</b>, photographs, or videos.</li> </ul> <p>Paper Format</p> <ul style="list-style-type: none"> <li>• <b>Associates should not print protected health information in their home. If a circumstance should arise requiring an associate to print at home the associate will need approval from their supervisor and the Privacy Officer.</b></li> <li>• <b>Disposal of documents containing protected health information should be done in EHN shredding bins. Documents should not be discarded in trash containers at home, a client's home or public businesses. All protected health information should be protected and stored in a secure area. Documents should also be protected from inadvertent destruction or alteration.</b></li> </ul>
---	--

<p><b>Safeguarding Confidential Information During Telecommuting, Page 25-</b> The safeguarding of protected health information was added to address employees authorized to telecommute.</p>	<p><b>1.10.4 Safeguarding Confidential Information During Telecommuting</b></p> <p>Although telecommuting can be an advantage for users and for the organization in general, it presents risks in the areas of confidentiality and the security of protected health information. Employees connected to EHN's network via a virtual private network become an extension of the wide area network and present additional environments that must be protected against the danger of cybersecurity threats. This arrangement also exposes the corporate as well as protected health information to risks not present in the traditional work environment. In addition to section 1.10.2 the following guidelines need to be followed during telecommuting.</p> <ul style="list-style-type: none"> <li>• Take necessary precautions to properly care for any equipment issued for use while engaging in telecommuting. Notify a supervisor immediately of any damaged or lost equipment. Return any equipment issued upon separation from employment.</li> <li>• Lock computer screen when stepping away from the computer when at home or a client's home. All computers will automatically lock after 3 minutes of inactivity. You can also manually lock a screen by simultaneously pressing <i>Windows Key+L</i>. Do not allow family members to use work equipment or access protected health information.</li> <li>• Transferring data to personal devices such as computers, tablets, or cell phones is prohibited. Protected health information should not be sent to personal emails or stored in the cloud or thumb drives. Protected health information should not be sent to or from family members devices or accounts.</li> <li>• Data entry in public locations is not recommended as computer screens can be viewed by individuals in the area of the computer screen.</li> <li>• Protected health information should be encrypted when sending to an individual that is not an associate of EHN (see Information Security Policy, Section 4.10 Use of Encrypted Email). Encryption can be waived only if a consumer requests that the protected health information not be encrypted. EHN associates cannot initiate the conversation about transmitting protected health information without encryption. If an EHN associate receives permission from a consumer to transmit protected health information without encryption the EHN Associate must advise the client of the risks associated with the transmission of unencrypted information. The associate should also document in the client record that they received permission from the consumer.</li> <li>• Disposal of documents containing protected health information should be done in EHN shredding bins. Documents should not be discarded in trash containers at home, a client's home or public businesses such</li> </ul>
---	--

	<p>as gas stations. All protected health information should be protected and stored in a secure area. Documents should also be protected from inadvertent destruction or alteration.</p>
<p><b>Consent for Uses and Disclosures Permitted, Page 32-</b>  Added legally authorized representative and child as the individuals that may receive the notice of privacy practices during their first visit to EHN.</p>	<p>Procedure</p> <p>At the time of consumer's, <b>authorized personal representative, or a child's</b> first visit to the organization consumers will be given the notice of privacy practices. The notice shall contain all permitted uses and disclosures that may be made without the consumer's authorization. Review section 1.17 for additional details on use and disclosure of protected health information for treatment purposes. Review section 1.18 for additional details on use and disclosure of protected health information for payment purposes. Review sections 1.19 for additional details on use and disclosure of protected health information for health care operations. Consumers will not be given the option to consent for treatment, payment, or health care operations. Authorization for disclosures is required for any other types of disclosure not covered by treatment, payment, or health care operations.</p>
<p><b>Use and Disclosure of Protected Health Information for Treatment Purposes, Page 33-</b> Identified whose protected health information this policy applies to when using or disclosing protected health information for treatment purposes; and when use and disclosure for treatment purposes applies.</p>	<p>Use and Disclosure of Protected Health Information for Treatment Purposes</p> <p>Emergence Health Network uses protected <b>health</b> information pursuant to its notice of privacy practices and under the guidance of the HIPAA privacy regulations for purposes of consumer treatment <b>and care coordination</b>. The use and disclosure of information for the purpose of treatment does not require specific authorization (see <b>section 1.33 authorization of use and disclosure</b>), <b>this applies to a consumer, an authorized personal representative, or a child.</b></p>



Mail Copies (complete address):

Pick-Up copies (location of pick-up):

Fax copies (attention to):

12. I also authorize the disclosure or receipt of my health information regarding (a selection is required to consent or deny the release of the following information):

Yes  No Alcohol or Substance Abuse Records

Yes  No HIV/AIDS Records

Yes  No Genetic Information (including Genetic Test Results)

13. Purpose of Receipt/Disclosure:

at my request  legal purposes  billing and claims

educational purposes  treatment/continuity of care

to verbally disclose the care and treatment I receive

other:

14. The persons or organizations receiving any Disclosure of this information will be prohibited by law from re-disclosing any information received based upon this consent and will be notified of that fact in every disclosure.

Consent:

Effective Date:

Expiration Date:

I understand that this permission may be revoked. I also understand that records disclosed before this permission is revoked may not be retrieved. Any person or organization that relied on this permission may continue to use or disclose records and protected health information as needed to complete work that began because this permission was given.

I DENY CONSENT (Revoke)

I understand that EHN is sensitive about client's trauma and realizes the effects it can

have. EHN encourages clients to participate in treatment decision making by giving them a voice and choice about the information that is shared with EHN and its staff. EHN promotes a trauma informed approach to its care and interactions with patients to reduce re-traumatization.

I am the person or personal representative of the person whose records will be used, disclosed, or exchanged. I give permission to use, disclose, and exchange records as described in this document.

I understand that Emergence Health Network (EHN) may share my health information in EHN's files with another medical provider to help with my treatment with that other provider with or without my permission as allowed under federal and state privacy laws (45 CFR 164.506(c)(4), Tex. Health and Safety Code 611.004(a)(7),

Tex. Health and Safety Code 81.103(b)(5)).

I understand that I do not have to give consent to share alcohol and/or substance abuse treatment information with my medical provider(s), but by authorizing disclosure on page one (1) of this form, I freely choose to do so. I also understand that I may revoke, at any time, my authorization for the medical provider(s) to have access to alcohol and/or substance abuse treatment information, however, other information regarding my treatment with EHN may be shared with the medical provider(s) as allowed under HIPAA and any other federal or state privacy laws. My decision to revoke this authorization shall only apply to information which has not already been

shared with the medical provider(s).

If there is any information in my medical record regarding current or past alcohol and/or substance abuse treatment, federal law prohibits EHN from sharing that information without my permission, unless in certain situations such as a medical emergency (42 CFR Part 2). The sharing of this information may be helpful to my medical provider(s) for my treatment.

I understand that my permission to share this information does not automatically mean that I have an alcohol or substance abuse problem, or that I have ever used or abused alcohol or drugs. Even though I may not have information in my medical record related to alcohol and/or substance abuse treatment, my permission to share this information will allow EHN to share my medical records quicker to my medical provider(s).

If I choose not to give permission to share alcohol and/or substance abuse treatment information, EHN will still provide my information to my medical provider(s), however, every document in my medical record will have to be reviewed to ensure that the substance and/or substance abuse treatment information is not shared.

I understand that the review of my medical record may require several hours and that an immediate turn-around cannot be guaranteed.

Please allow 10 business days for your request

<b>Client Signature:</b>		<b>Date:</b>	
<b>Parent/Guardian Signature:</b> <i>(if not applicable, enter "N/A")</i>		<b>Date:</b>	
<b>LAR Signature:</b> <i>(if not applicable, enter "N/A")</i>		<b>Date:</b>	
<b>Staff Name:</b>		<b>Title:</b>	

**For Office Use ONLY:**

Process Request (allow 10 business days)       Upload into client's chart ONLY

