HIPAA Privacy Policies & Procedures

Protection of Individually Identifiable Health Information

Table of Contents

HIPAA: GENERAL STANDARDS

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this General Standards policy as a foundation for the Company's Privacy Program.

POLICY AND PROCEDURE:

1. The Company will disclose its practices related to the use and disclosure of PHI in its Notice of Privacy Practices.

    **Note: Facility based providers will use and abide by the Facility's Notice of Privacy Practices and HIPAA Privacy policies.

2. The Company will only use and disclose information in the most appropriate fashion, defined by the limitations of job function and "need to know" basis, as referenced in Policy 4 – Minimum Necessary/Need to Know.

3. The Company will verify the identity of all individuals prior to the release of PHI.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: DEFINITION OF PROTECTED HEALTH INFORMATION (PHI) / DE-IDENTIFICATION OF PHI

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Definition of Protected Health Information (PHI) / De-Identification of PHI policy to define the term "Protected Health Information" ("PHI") for use in these policies, and to define the data elements considered to classify patient data as "identifiable."

POLICY:

A) Protected Health Information or PHI, (also known as "individually identifiable information"), as used in these policies, is defined as a subset (record or transmission) of health information, including demographic information collected from an individual. It is created or received by a health care provider (including the Company), health plan, employer, or health care clearinghouse. It relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. Additionally, the information identifies the individual or can be used to identify the individual.

The following is a list of data elements that are considered to be an identifier of an individual (*the data elements listed below may relate to relatives, employers, or household members of the individual*):

(1) Names;
(2) All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code;
(3) All elements of dates (except year) for dates directly related to an individual, including 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;
(4) Telephone numbers;
(5) Fax numbers;

(6) Electronic mail addresses;
(7) Social security numbers;
(8) Medical record numbers;
(9) Health plan beneficiary numbers;
(10) Account numbers;
(11) Certificate/license numbers;
(12) Vehicle identifiers and serial numbers, including license plate numbers;
(13) Device identifiers and serial numbers;
(14) Web Universal Resource Locators (URLs);
(15) Internet Protocol (IP) address numbers;
(16) Biometric identifiers, including finger and voice prints;
(17) Full face photographic images and any comparable images;
(18) Any other unique identifying number, characteristic, or code.

B) Health information that does not identify a patient is not PHI and does not to be treated consistent with the principles set forth in these policies. Health information does not identify the patient if:
   (1) The identifiers listed in paragraph A of this policy are removed from the record or transmission of health information; or
   (2) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:
      (a) determines that the risk is very small that the information could be used, alone or in combination, with other reasonably available information by an anticipated recipient to identify a patient who is a subject of the information; and
      (b) documents the methods and results of the analysis that justify such determination.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: MINIMUM NECESSARY / NEED TO KNOW

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Minimum Necessary / Need to Know policy to present the primary principle defining how PHI will be used and disclosed throughout the organization.

POLICY:

A) Access to information in the possession of or under the control of the Company must be provided based on the "need-to-know". In other words, employees and business associates will be given access to PHI and/or PHI will be disclosed to them only when there is a legitimate business need for the information. Teammates and business associates must not attempt to access PHI unless they have been granted appropriate access rights and have a clear business reason to do so.

B) Accordingly, the Company's approach to ensuring patient privacy and data security is to implement policies and procedures and to employ technological tools, when possible, that restrict access and uses of PHI based on the specific roles of its work force, including but not limited to employees, contractors, physicians, volunteers, other temporary workers, and business associates.

C) The Company will limit access to PHI to the "minimum necessary" to achieve the intended purpose of the use or disclosure of PHI. The Company will establish specific policies and procedures to guide any routine uses or disclosures of PHI that are ***not*** related to treatment, associated payments, or any other routine health care operation related to the patient care.

D) The Company will review non-routine requests for information on an individual basis, determine whether the PHI requested is the minimum necessary, and respond appropriately.

E) The Company will ***not*** apply "minimum necessary" standards to requests for information from the patient to any disclosures required by the Secretary of U.S. Department of Health and Human Services for the purposes of determining whether the Company is in compliance with HIPAA, nor to any disclosures required by Federal, State, or local laws.

F) The Company will rely on a requested disclosure as the minimum necessary for the stated purpose when:

(1) Making disclosures to public officials as required by law;
(2) The information is requested by another health care provider, health plan, or clearinghouse;
(3) The information is requested by a researcher, provided the requirements outlined in Policy 19 – Uses and Disclosures of Protected Health Information for Research are met; or
(4) The information is requested by a professional who is a member of the Company's work force or is a business associate, who represents that the requested information is the minimum necessary to perform a service on behalf of the Company.

G) The Company will also limit and monitor its requests for information from another health care agency, health plan, or clearinghouse. The Company will request only the minimum necessary protected health information required to achieve the purpose of a particular use or disclosure using the standard corporate "Authorization for Release of Medical Information" unless the request is made on a recurring and routine basis. In this case, the Company will rely upon its policies and procedures to ensure the appropriate use and disclosure of PHI.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: NOTICE OF PRIVACY PRACTICES

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Notice of Privacy Practices policy to ensure that individuals are provided with the information needed to clearly understand how their health information can be used or disclosed, their rights under HIPAA with respect to their health information, and how they can gain access to their health information. In addition, this policy establishes the administrative procedures regarding the maintenance of the notice.

POLICY:

Individuals have a right to adequate notice of the uses and disclosures of protected health information that may be made by the Company and of the individual's rights and the Company's legal duties with respect to protected health information. NOTE: Facility-based providers will use and abide by the Organized Health Care Arrangement's Joint Notice of Privacy Practices.

Provision of Notice

The Notice of Privacy Practices ("Notice") is made available as follows:

A) A written copy is given to all patients the **first** time they receive treatment or upon first service (*See* current Notice of Privacy Practices form available on website). It is not necessary to provide a written copy of the Notice at subsequent visits or upon subsequent delivery of services.

B) A copy of the Notice must be posted prominently in the waiting room or admissions area, if applicable for your department, where it can easily be read, as well as on the website, if one is maintained.

C) Printed copies of the Notice are made available to any person (whether or not a patient) who requests a copy.

D) Copies of the Notice may be provided electronically as long as the patient is advised that he or she may request a written copy as well.

Acknowledgement of Receipt of Notice

The first time the patient receives treatment or services, the patient or the patient's authorized representative is asked to sign a receipt acknowledging that the Notice was provided. If the person's signature cannot be obtained, document the good faith attempt to obtain the acknowledgement.

After the patient signs and dates the Notice, the staff gives a copy of the Notice to the patient and files the original copy in the medical record or at the service location of treatment.

Emergencies

In an emergency, it is not necessary to provide the Notice or obtain acknowledgement until after the emergency has been resolved.

Revisions to Notice

Any changes to the Company Notice of Privacy Practices must be approved by the Privacy Official and Chief Compliance Officer to assure that the Notice contains all required elements and accurately reflects federal and state law. Before the Company may change its privacy practices in any way that is inconsistent with the current description, the Notice is revised to describe the change. The effective date of the new Notice is printed on the Notice and cannot be retroactive. Any time the Notice is revised, the revised copy must be posted prominently, and written copies must be made available upon request. If significant changes are made to the Notice, a written copy on the first visit or first service must be provided, and patient signature must be obtained as proof a copy was provided. Subsequent visits will not require a written copy be handed out unless patient requests a copy.

Retention

The Company must retain copies of the Notices issued by the Company for six (6) years from the date of its creation or the date when it last was in effect, whichever is later.

Joint Notice of Privacy Practices

The Company may participate in an organized health care arrangement that has established a Joint Notice of Privacy Practices ("Joint Notice"). In this case, the Company may rely on the Joint Notice provided that:

A) The Company agrees to abide by the terms of the Joint Notice with respect to PHI created or received by the Company as part of its participation in the organized health care arrangement.

B) The Joint Notice meets the Company's requirements for its Notice of Privacy Practices; and
   (1) Describes with reasonable specificity the providers or agencies, or classes of providers or agencies, to which the Joint Notice applies;
   (2) Describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the Joint Notice applies; and
   (3) If applicable, states that the providers or agencies participating in the organized health care arrangement will share PHI with each other, as necessary, to carry out treatment, payment, or health care operations relating to the organized health care arrangement.

C) The providers or agencies included in the Joint Notice must provide the Joint Notice to patients in accordance with the Company's policies.

Contact for Questions

If a teammate has any questions or is uncertain about the requirements of this policy, such teammate should contact the Privacy Official.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: DISCLOSING PROTECTED HEALTH INFORMATION FOR HEALTHCARE OPERATIONS

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Disclosing Protected Health Information for Healthcare Operations policy to inform teammates of the authority provided to them under HIPAA regarding the use and/or disclosure of protected health information for health care operations.

POLICY:

Use for Health Care Operations

The protected health information of the Company's patients may be used or disclosed for the health care operations of the Company in accordance with this policy.

The Company may use or disclose an individual's protected health information without an authorization for the purpose of health care operations.

Health care operations means activities related to carrying out and monitoring the internal functions of the Company, including, but not limited to, quality assessment, review of care, records management, training and education, resolution of internal grievances, certification and licensing activities, business management, general administrative functions, planning and development, auditing of Company activities, conducting or arranging for legal services, patient satisfaction surveys, and similar activities.

Optional Consent to Use Health Information for Health Care Operations

Except as required by state law, it is not mandatory to obtain written consent/authorization to use or disclose the patient's health information for health care operations purposes. (However, an "informed consent for treatment," disclosing the risks and benefits of a proposed procedure, is still required.)

Minimum Necessary Access

Information that is used and shared for health care operations purposes is subject to minimum necessary disclosure rules. Only those workforce members who have been granted appropriate authority are allowed to use or review patient information for health care operations and may access only the information needed to carry out their duties.

Use of Business Associates for Health Care Operations Purposes

Outside parties such as auditors, management companies, attorneys, accountants, and others may assist in carrying out the Company's health care operations. If these parties use or disclose patient health information when assisting the Company with health care operations, they must have a business associate contract in accordance with the Company's separate policy on business associates.

Disclosures to Other Providers and Health Plans for Their Health Care Operations Purposes

Patient information may be disclosed for the health care operations purposes of other providers and health plans, provided that the following are met:

A) The other provider or health plan is covered by the HIPAA privacy regulations; and

B) The other provider or health plan has a current or prior relationship with the patient, and

C) The information is being sought for purposes related to quality assessment or evaluation of care and competence or is being sought for the purpose of health care fraud and abuse detection or compliance.

No Log of Disclosure Required

Disclosures for health care operations do not need to be recorded in the patient's Protected Health Information Disclosure Log.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: DISCLOSING PROTECTED HEALTH INFORMATION FOR TREATMENT

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Disclosing Protected Health Information for Treatment policy to inform teammates of the authority provided to them under HIPAA regarding the use and/or disclosure of protected health information for treatment purposes.

POLICY:

Use for Treatment

The protected health information of the Company's patients may be used or disclosed for treatment in accordance with this policy.

The Company may use or disclose an individual's protected health information without an authorization for the purpose of treatment.

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers. Treatment includes not only the direct provision of medical treatment, services, or products, but also consultations between providers, the referral of a patient for health care from one health care provider to another, and the coordination or management of the patient's health care by a health care provider and a third party.

Optional Consent to Use Health Information for Treatment

Except as required by state law, it is not mandatory to obtain written consent/authorization to use or disclose the patient's health information for treatment purposes. (However, an "informed consent for treatment," disclosing the risks and benefits of a proposed procedure, is still required.)

Internal Access by Company Professionals

The Company's clinicians may request and be given access to the complete health records of any Company patients they are treating or have previously treated. Support staff who are assisting in such treatment may also have access to the patient's health records in order to assist in the patient's treatment.

Contact the Privacy Officer if a Company physician or other professional seeks access to the record of a patient with whom he or she does not have a treatment relationship.

Disclosures to Outside Treatment Providers

Outside physicians and other health care providers involved in treating the patient, including hospitals, labs, pharmacies, nursing homes, and similar providers, may be given access to all health information about the patient, including the complete record if requested. If the record is extensive, you may contact the treatment provider to see if he or she would prefer to receive only selected portions of the record. If the patient has requested and been granted a restriction on disclosures to a particular provider, do not release the information to that provider except in an emergency. (For further information regarding requests for restrictions on disclosures, *see* Policy 25 – Restriction of Use of Disclosure)

Purposes Related to Treatment

Patient information may be shared with treatment providers in accordance with this policy as necessary to arrange for appointments, referrals, diagnostic tests, consultations, management and coordination of care, determinations of suitability for services, and similar services directly related to treatment.

Verification of Treatment Relationship

If the health care provider requesting the health information is not known to the Company, the provider's identity must be verified and documented. This may be accomplished by calling the person back at an official phone number or asking the person to fax the request on official letterhead of the provider they are representing. If necessary, contact the patient directly to confirm that the requesting provider is involved in the patient's treatment. If doubts still exist, contact the Privacy Official for a determination of further actions needed.

No Log of Disclosure Required

Disclosures for treatment do not need to be recorded in the patient's Protected Health Information Disclosure Log. For future reference, however, any treatment disclosures made to persons outside the Company should be noted in the patient's record and should indicate what information was disclosed, by whom, to what person, how that person is involved in the patient's treatment, and the date of disclosure.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: DISCLOSING PROTECTED HEALTH INFORMATION AS REQUIRED BY LAW

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Disclosing Protected Health Information as Required by Law policy to provide guidance to teammates regarding the procedures to be followed when using or disclosing protected health information as required by law.

POLICY:

Disclosures Required by Law

State and federal laws and regulations may mandate certain uses or disclosures of patient health information. For example, reports of child abuse are required under the laws of most states. If the law or regulation can be enforced by an official government agency, it is deemed to be required by law. (This does not include private contractual agreements between parties.) The Company may use or disclose patient information for purposes required by law in accordance with applicable state and federal laws.

Overlap with Other Policies

Many uses and disclosures required by law are also covered by other policies, such as the policies on public health activities and health oversight. Other than the exceptions listed below, if a use or disclosure is required by law and also falls under another policy, the Company may follow either this policy or the other applicable policy in determining how to use or disclose the health information.

Exception: Uses and Disclosures for Reporting Adult Abuse, Neglect, and Domestic Violence

If state or federal law requires a use or disclosure for reporting adult abuse, neglect, or domestic violence, the Company must follow the procedures described in the separate policy on reports of adult abuse, neglect, and domestic violence (*See* Policy 12 – Disclosing Protected Health Information About Victims of Abuse, Neglect, or Domestic Violence).

Exception: Uses and Disclosures for Judicial or Administrative Proceedings

If state or federal law requires a use or disclosure for judicial or administrative purposes (e.g., in response to subpoenas and court orders), the Company must follow the procedures described in the separate policy on judicial and administrative proceedings (*See* Policy 10 – Disclosing Protected Health Information for Judicial and Administrative Release).

Exception: Uses and Disclosures for Law Enforcement

If state or federal law requires a use or disclosure for law enforcement purposes (e.g., to report certain wounds or injuries, or in response to grand jury subpoenas), the Company must follow the procedures described in the separate policy on disclosures for law enforcement purposes (*See* Policy 11 – Disclosing Protected Health Information to Law Enforcement).

Logging of Disclosure

All disclosures required by law must be logged in accordance with the separate policy regarding accounting of disclosures (*See* Policy 35 – Content of Accounting of Disclosures).

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: DISCLOSING PROTECTED HEALTH INFORMATION ABOUT DECEDENTS

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Disclosing Protected Health Information About Decedents policy to provide teammates with guidance regarding allowable uses and disclosures of the protected health information of deceased patients.

POLICY:

Treatment of Health Records of Deceased Patients

The Company may, under certain circumstances, disclose the protected health information of deceased patients.

The health information of a deceased patient is subject to the same privacy protections as the health information of living patients until the person has been deceased for fifty (50) years. After fifty (50) years, it is NOT considered protected health information.

Personal Representative

The executor or administrator of the patient's estate has the right to exercise the privacy rights of the patient. This includes the right to inspect and obtain copies of the patient's health records, request amendments, and obtain an accounting of disclosures.

Allowable Disclosures

To the extent allowed by applicable state laws, the deceased patient's health information may be released as follows:

A) To medical examiners or coroners for the purpose of identifying the deceased person, determining a cause of death, or other duties as authorized by law.

B) To funeral directors as necessary to carry out their duties.

C) To organ procurement agencies for the purpose of facilitating organ, eye, or tissue donation and transplantation, provided that such disclosure was authorized by the patient, the patient's personal representative, or is otherwise required or authorized by law.

D) To authorized officials or agencies carrying out public health activities, health oversight, law enforcement, research, or other purposes for which an authorization is not required, provided that the disclosure complies with the applicable requirements of the Company's separate policies regarding such disclosures.

Logging of Disclosure

All disclosures for purposes other than for treatment, payment, health care operations, or as authorized by the patient's personal representative must be logged in accordance with the separate policy regarding accounting of disclosures (*See* Policy 35 – Content of Accounting of Disclosures).

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: DISCLOSING PROTECTED HEALTH INFORMATION FOR JUDICIAL AND ADMINISTRATIVE RELEASE

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Disclosing Protected Health Information for Judicial and Administrative Release policy to provide teammates with guidance regarding the disclosure of protected health information for the purpose of a judicial or administrative proceeding.

POLICY:

Orders of Court or Administrative Tribunal

Patient health information may be released in response to a valid court order or an order from an administrative tribunal.

A valid court order is one that has been specifically approved by the court and signed by the judge. It does not include a subpoena automatically issued by a clerk of the court at the request of an attorney. An "administrative tribunal" is a specialized court associated with an administrative agency, such as the IRS or Social Security Administration, rather than a general court that hears a variety of types of cases. An order from an Administrative Law Judge ("ALJ") should be treated like an order of any other court. Contact legal counsel if there are any doubts about the validity of an order from a court or administrative tribunal.

Subpoenas, Discovery Requests, and Other Legal Process

Patient health information may be released as follows:

A) The patient provides a written and dated authorization to release the information to the requesting party. The authorization must meet the requirements set forth in the Company's separate policy on authorizations for the release of information (*See* Policy 39 – Authorization Requirements).

B) The subpoena or request is accompanied by a valid order from a court or administrative tribunal, as described above.

C) Satisfactory assurance has been obtained from the party seeking the information that either (1) acceptable notice has been given to the patient, or (2) an appropriate protective order has been obtained.

D) The subpoena requires the information to be disclosed for law enforcement or investigation purposes, and meets the requirements listed in the Company's separate policy regarding disclosures for law enforcement purposes (*See* Policy 11 – Disclosing. This includes grand jury subpoenas and subpoenas issued by government attorneys on behalf of local, state, and federal enforcement agencies.

Scope of Disclosure

Release only the information expressly authorized by the order or requested by the subpoena.

Logging of Disclosure

All disclosures in response to a court order, administrative tribunal order, subpoena, discovery request, or other legal process must be logged in accordance with the separate policy regarding accounting of disclosures (*See* Policy 35 – Content of Accounting of Disclosures).

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: DISCLOSING PROTECTED HEALTH INFORMATION TO LAW ENFORCEMENT

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Disclosing Protected Health Information to Law Enforcement policy to provide teammates with guidance regarding proper procedure for disclosing protected health information to law enforcement.

POLICY:

Law Enforcement Agencies and Officials

Law enforcement agencies and officials may be provided with protected health information only in accordance with this policy.

A "law enforcement official" includes any officer or employee of a city or municipality, a state, the United States, or an Indian tribe, who is empowered to investigate a potential violation of a law or to prosecute or conduct a judicial proceeding arising from an alleged violation of law. Law enforcement officials include, but are not limited to, local police, state troopers, FBI agents, and representatives of the federal Office of the Inspector General who are investigating a potential Medicare fraud violation. They also include grand juries, district attorneys, US attorneys, other prosecuting entities who are investigating or prosecuting a crime, military police ("MPs") who are conducting an investigation into a crime committed by a member of the military, and judges who issue court orders for the disclosure of information needed in an investigation.

Required By Law

Protected health information may be disclosed to law enforcement agencies to make reports that are required by law, including the following:

A) To report suspicious injuries, such as an injury by knife, pistol, gun, or other "deadly weapon," or caused by poisoning or suffocation.

B) To report suspected abuse or neglect.

Response to Legal Process

Protected health information may be disclosed in response to legal process or summons, as follows:

A) To comply with a court order or court-ordered warrant ordering disclosure to the law enforcement agency.

B) To comply with a subpoena or summons issued by a judicial officer rather than by a private attorney. If the subpoena was issued by a private attorney, or if it calls for the information to be provided to someone other than a law enforcement official, refer to the policy on disclosures in response to subpoenas (*See* Policy 10 – Disclosing Protected Health Information for Judicial and Administrative Release).

C) To comply with a grand jury subpoena.

D) Pursuant to an official request from a law enforcement agency (e.g., a request for information from an enforcement agency of the federal government, such as the Bureau of Alcohol, Tobacco and Firearms). Provide the agency with the letter entitled "Letter Regarding Law Enforcement Requests" (*see* attached form below) which must be completed and returned before the information may be released.

Suspects, Fugitives, Material Witnesses, or Missing Persons

Protected health information may be provided to law enforcement agencies and officials who are attempting to identify or locate a suspect, fugitive, material witness, or missing person. The information may be provided in response to requests by a properly identified law enforcement officer or in response to a public bulletin issued by a law enforcement agency.

A) Only the following information may be provided:

(1) Name and address
(2) Date and place of birth
(3) Social security number
(4) ABO blood type and Rh factor
(5) Type of injury
(6) Date and time of treatment
(7) Date and time of death, (if applicable)
(8) Description of any distinguishing physical characteristics of the patient, including height, weight, gender, race, hair and eye color, facial hair, scars, and tattoos.

B) Do <u>not</u> disclose any information related to DNA or a DNA analysis, dental records, samples or analysis of body fluids or tissues, or any other information beyond the information listed above, unless the officer presents a warrant, subpoena, or court order meeting the requirements of *Response to Legal Process* section, above.

Victims of Crime

If the patient is suspected of being the victim of an alleged crime, patient information may be disclosed to law enforcement officials as follows:

A) A conscious, competent patient must be asked if the information may be disclosed to law enforcement officials. Document the time, date, and name of the persons who witnessed the patient's agreement or refusal. If possible, obtain an "Authorization" form signed by the patient (*See* Policy 13 – Personal Representatives and form attached thereto).

B) If the patient is not competent, the patient's legally authorized representative may agree to the disclosure of the information, in which case they should sign an "Authorization" form (*See* Policy 13 – Personal Representatives regarding who qualifies as a legally authorized representative and form attached thereto). If no legally authorized representative is available, try to find a family member who may agree to contact law enforcement officials directly.

C) In an emergency, or when no authorized representative or family member is available, the protected health information may be disclosed only if the law enforcement officer signs the statement entitled "Official Statement Regarding Need for Information Regarding Possible Victim of Crime" (*See* attached form below) and either the Privacy Official or the patient's attending physician determine that disclosure is in the patient's best interests. The determination must be documented.

Deaths

Suspicious deaths, including related protected health information, may be disclosed to law enforcement agencies and officials if the death is suspected of being the result of criminal conduct. The Privacy Official is responsible for reviewing the circumstances and determining that disclosure should be made. The determination must be documented.

Criminal Activity on Premises

Evidence of suspected criminal conduct occurring on the Company's premises, including related protected health information, may be disclosed to law enforcement agencies and officers. The Privacy Official is responsible for reviewing the circumstances and determining that disclosure should be made. The determination must be documented.

Criminal Activity Off-Site

An individual health care provider may disclose information to law enforcement officers that he or she learned while responding to a medical emergency off-premises, if necessary to alert them to the commission or nature of a crime, the location or victims of a crime, or the identity, description, or location of the perpetrator of a crime.

Reports to Avert a Serious Threat

A report may be made to law enforcement authorities to help identify or apprehend an individual under the following circumstances:

A) Because the individual made a statement admitting participation in a violent crime that is reasonably believed to have caused serious physical harm to the victim (in which case the only information that may be disclosed is the individual's statement and the patient information described in the *Suspects, Fugitives, Material Witnesses, or Missing Persons* section above), or

B) Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.

Verification of Identity

Before disclosing protected health information to a law enforcement officer or agency, the officer's or agency's identity must be verified and documented. If the person is a police officer, ask to see his or her badge and record the badge number. For persons who do not have a badge, obtain their business card or other proof of their credentials. All requests received in writing should be on official letterhead. If any doubt exists regarding the validity of a request, contact the Privacy Official for further determination.

Logging of Disclosure

All disclosures to law enforcement agencies and officials must be logged in accordance with the separate policy regarding accounting of disclosures (*See* Policy 35 – Content of Accounting of Disclosures).

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

LETTER REGARDING LAW ENFORCEMENT REQUESTS

Date: ___________

VIA FACSIMILE OR HAND-DELIVERY

____
____
____

Dear Sir or Madam:

We have been asked to provide your agency with certain information that may be protected under state and federal health privacy regulations. A copy or summary of your agency's request is attached.

Before any information may be released, we must obtain the agency's certification that all of the following statements are true:

1. The information being sought is relevant and material to a legitimate law enforcement inquiry;
2. The request for such information is specific and limited to the purpose for which the information is sought; and
3. The agency could not conduct the investigation using de-identified[1] information.

Thank you for your attention to this matter. Please complete the certification below and return it to us with an official cover page on agency letterhead. If you have any questions, please do not hesitate to call me at ________________________.

Sincerely,

Privacy Officer for ____________________
[Name of Center]

[1] "De-identified" means the removal of all information that could be used to identify the individual, either directly or in combination with other known information, and includes the patient's name, street address, city, county zip code, date of birth (except for year), date of treatment (except for year), telephone, fax, e-mail, Social Security Number, medical record number, insurance or account numbers, photographs, and similar unique characteristics, numbers, and codes.

LETTER REGARDING LAW ENFORCEMENT REQUESTS

CERTIFICATION

On behalf of ___________________________________[name of agency], I hereby certify that the above statements are true and correct.

Signed: ______________________________________ Date: __________________________

Print name: ___________________________________

Title: ____ Telephone: _____________________

Address: ______________________________________

____

Envision HEALTHCARE

OFFICIAL STATEMENT REGARDING NEED FOR INFORMATION REGARDING POSSIBLE VICTIM OF CRIME

(To be completed by authorized representative of law enforcement agency)

Name of Patient: ____

Date of Birth: ____________________

I hereby certify that the information requested regarding the above-named patient is needed to determine whether a violation of law committed by someone else has occurred, and the information is not intended to be used against the victim.

I also certify that the investigation would be materially and adversely affected by waiting until the patient is able to agree to the disclosure.

Signed: ________________________________ Date: ________________________________

Print Name: ____________________________ Telephone: ___________________________

Title: __________________________________ Supervisor: ___________________________

Badge Number: _________________________ Name/Address of Law Enforcement Agency:

____

____

____

HIPAA: DISCLOSING PROTECTED HEALTH INFORMATION ABOUT VICTIMS OF ABUSE, NEGLECT, OR DOMESTIC VIOLENCE

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Disclosing Protected Health Information About Victims of Abuse, Neglect, or Domestic Violence policy to provide teammates with guidance regarding the procedures to be followed when disclosing protected health information about an adult victim of abuse, neglect, or domestic violence.

POLICY:

Allowable Disclosures to Government Authorities

If, in the documented professional opinion of a licensed professional affiliated with the Company, an adult patient reasonably appears to be the victim of abuse, neglect, or domestic violence, the Company may disclose protected health information to a government authority, such as a social service or protective service agency, that is authorized by law to receive such reports, only if one of the following circumstances applies:

A) The disclosure is required by law and only that information required by and relevant to the law is disclosed.

B) The individual has agreed to the disclosure. The agreement may be given orally as long as it is documented in the patient's record.

C) The disclosure is expressly permitted by law, and either (i) in the documented opinion of a licensed professional, the disclosure is necessary to prevent serious harm to the patient or other potential victims, or (ii) the patient is unable to agree to the disclosure and a law enforcement or other official signs the form entitled "Official Statement Regarding Need for Information Regarding Possible Victim of Adult Abuse, Neglect, or Domestic Violence" (*See* attached form below).

Informing the Patient

The patient must be informed promptly, either verbally or in writing, when a report has been or will be made, except under the following circumstances:

A) A licensed professional affiliated with the Company, in the exercise of professional judgment, documents his or her belief that informing the patient would place him or her at risk of serious harm; or

B) The patient is not capable of being informed, and his or her personal representative may be responsible for the abuse, neglect, or other injury, and therefore informing the personal representative would not be in the best interests of the patient, as determined and documented by a licensed professional affiliated with the Company.

Logging of Disclosure

All disclosures made in accordance with this policy must be logged in accordance with the separate policy regarding accounting of disclosures (*See* Policy 35 – Content of Accounting of Disclosures).

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

.

OFFICIAL STATEMENT REGARDING NEED FOR INFORMATION REGARDING POSSIBLE VICTIM OF ADULT ABUSE, NEGLECT, OR DOMESTIC VIOLENCE

(To be completed by law enforcement official or other public official authorized to receive reports of suspected abuse, neglect, or domestic violence)

Name of Patient: ___________________________

I hereby certify that the information requested regarding the above-named patient is needed to investigate possible abuse, neglect, or domestic violence, and the information is not intended to be used against the victim.

I also certify that an immediate enforcement activity depends on the disclosure and that the enforcement activity would be materially and adversely affected by waiting until the patient is able to agree to the disclosure.

Signed: ___________________________________ Date: ___________________________

Print Name: ______________________________ Telephone: _____________________

Title: ___________________________________

Badge Number (if applicable): ____

Name/Address of Agency: ____

____

HIPAA: PERSONAL REPRESENTATIVES

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Personal Representatives policy to define a legitimate patient representative who is authorized to receive a patient's medical information. Additionally, this policy will clearly identify the Privacy Rights afforded to a personal representative on a patient's behalf, identify those persons who may be designated as a personal representative on a patient's behalf, and establish a process for identity verification of personal representatives.

POLICY:

Definition

A) For the purposes of these policies, the Company will treat a person as a personal representative of a patient, if under applicable law, a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care.

B) The Company will also treat a person as a personal representative of a patient, if under applicable law, a parent, guardian, or other person acting *in loco parentis* has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care.

C) An individual will not be a personal representative of an unemancipated minor, when the minor has the authority to act as an individual, if:

(1) The minor consents to health care service; no other consent to such health care service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as the personal representative;

(2) The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting *in loco parentis*, and the minor, a

court, or another person authorized by law consents to such health care service; or

(3) A parent, guardian, or other person acting *in loco parentis* assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

Who Has Authority

A competent adult patient has authority to exercise his or her rights regarding the use or disclosure of protected health information. In addition, other persons described in this policy may serve as the patient's personal representative with authority to exercise, on the patient's behalf, the patient's rights regarding the use or disclosure of protected health information.

Privacy Rights

The privacy rights subject to this policy are the right to (a) receive a notice of the Company's privacy policies; (b) inspect and obtain copies of the Company's records containing the patient's protected health information; (c) amend the information; (d) obtain an accounting of disclosures of the information; (e) request restrictions on the use or disclosure of the information; and (f) receive confidential communications from the Company.

Adult Patients

For adult patients (age 18 or older), only the following persons have authority to exercise the patient's privacy rights:

A) The patient, if not incompetent.

B) A person who has been appointed by the patient under a valid durable power of attorney for health care decisions or under any other valid power of attorney to the extent that the document describes such rights.

C) The patient's court-appointed guardian, conservator, or administrator.

D) The patient's spouse and relatives, if authorized under state law to make treatment decisions on the patient's behalf.

E) The executor or administrator of a deceased patient's estate.

Minor Patients

For minor patients (under 18 years of age), only the following persons have authority to exercise the patient's privacy rights:

A) The minor patient if, under state law, the minor is deemed "emancipated" or is otherwise entitled to make treatment decisions without parental involvement.

B) The minor patient's court-appointed guardian, conservator, or administrator.

C) The minor patient's parents, unless state law authorizes the minor to obtain the treatment without parental involvement, and the minor sought and consented to the treatment independently. (NOTE: Even if the parents do not have authority to exercise the minor's privacy rights, they may have the right to review the minor's records. *See* Policy 14 – Disclosing Protected Health Information for Minors to Parent or Legal Guardian regarding disclosures of a minor patient's health information to his or her parents.)

D) Other persons authorized under state law to make treatment decisions on the patient's behalf.

E) The executor or administrator of a deceased minor patient's estate.

Verification of Identity and Authority

If the person is not known to the Company, the person's identity and authority must be verified and documented before the person may exercise any of the patient's privacy rights. The patient's confirmation of a personal representative's identity and authority is adequate. If given verbally, rather than in writing, the confirmation must be documented in the record. Other acceptable verification of identity includes:

A) Driver's license

B) Birth certificate

C) Passport

D) Social Security card

E) Photo ID (with another piece of verification if possible)

F) Any other verification deemed reasonable by the Privacy Official

Acceptable verification of relationship or legal authority includes, but is not limited to, relevant official documents, including birth certificates, marriage certificates, passports, guardianship papers, and attorney-in-fact documents.

If any doubts exist regarding the person's identity or authority, or about the appropriateness of the verification presented, contact the Privacy Official.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: DISCLOSING PROTECTED HEALTH INFORMATION FOR MINORS TO PARENT OR LEGAL GUARDIAN

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammate" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Disclosing Protected Health Information for Minors to Parent or Legal Guardian policy to provide guidance to teammates regarding the appropriate circumstances and procedures for the disclosure of a minor's protected health information to their parent(s) or legal guardian.

POLICY:

The protected health information of minor patients (under age 18) may be used or disclosed to the minor patient's parent(s) or legal guardian only in accordance with this policy.

Parental Involvement

In most cases, the minor patient's custodial parent(s) or guardian(s) are involved in obtaining treatment for the minor and will have consented to treatment and assumed responsibility for payment. In that case, the parent(s) or guardian(s) has the right to exercise the minor patient's privacy rights, including the right to review the minor's protected health information.

Rights of Non-Custodial Parent

State law may allow non-custodial parents to review the medical records of their child, but they generally do not have the right to exercise the minor patient's other privacy rights (such as requesting amendments, accountings, or restrictions on disclosure). Unless prohibited by state law or by a court order, a non-custodial parent may be provided with a copy of the child's medical records upon written request and payment of copying fees. If the non-custodial parent is responsible for paying for the child's treatment, the non-custodial parent may also have access to the child's payment records. If the non-custodial parent is not known to the Company, obtain and document verification of his or her identity and relationship to the child. Contact the Privacy Official if there are doubts about the non-custodial parent's right to see the child's records.

Rights of Stepparent

A stepparent generally does not have the right to have access to the child's protected health information unless given such rights by a court. However, if the stepparent is known to be actively involved in a minor patient's health care treatment, the stepparent may be given access to those parts of the record that are directly relevant to the care being provided by the stepparent (*See* Policy 15 – Disclosing Protected Health Information to Family/Friends/Caregivers).

Verification of Identity and Relationship

If the person is not known to the Company, obtain and document verification of the person's identity and relationship to the child. If there is any doubt about the person's identity and relationship to the child, contact the Privacy Official.

Treatment Obtained by Minor without Parental Involvement

If the minor patient obtained the treatment independently, without the involvement of a parent or guardian, and is either "emancipated" or otherwise entitled under state law to consent to such treatment, disclosures to the minor's parents shall be made only under the following circumstances:

A) State law does not prohibit disclosure of the information to the minor's parents, and the treating practitioner determines that it is appropriate to release the information to the parents; or

B) The minor patient has been advised, and does not object, that his or her parents may be billed for the services unless other satisfactory payment arrangements are made. (This allows the minor to elect not to receive the treatment if he or she cannot make payment arrangements and does not want a bill sent to the parents.) The minor's agreement should be documented in the record.

Logging of Disclosure

If the parent is acting as the minor patient's personal representative, there is no need to log the disclosure. If the parent does not have such authority but is being given the records because the treating practitioner determines that the release is appropriate, the disclosure must be logged in accordance with the separate policy regarding accounting of disclosures (*See* Policy 35 – Content of Accounting of Disclosures).

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: DISCLOSING PROTECTED HEALTH INFORMATION TO FAMILY / FRIENDS / CAREGIVERS

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Disclosing Protected Health Information to Family / Friends / Caregivers policy to provide guidance to teammates regarding the appropriate process for disclosing protected health information to individuals other than the subject of the information.

POLICY:

Under the circumstances described below, relevant health information about the patient may be shared with the patient's family members, other relatives, close personal friends, or other persons identified by the patient.

Disclosures When the Patient Can Agree or Object

If the patient is accompanied by another person, do not discuss or disclose the patient's protected health information in front of the other person until the patient has been given the opportunity to agree or object. Ask the patient, "Would you prefer that we discuss these issues privately?" and if the patient says 'yes,' the other person should be asked to remain in another room or area of the facility. Document the patient's response in the patient's record, and sign and date the entry.

Disclosures When the Patient Is Not Able to Agree or Object

If the patient is not present, or cannot be given the opportunity to agree or object because of incapacity or an emergency situation, a professional determination should be made as to whether it is reasonable and in the patient's best interests to disclose the information. For example, it is reasonable to allow the patient's family member or friend to pick up the patient's prescription, medical supplies, or x-rays, as long as the person's identity is known to the Company. If the person is not known to the Company, verify and document the person's identity and authority.

Notification Purposes

Relevant patient health information may be used or disclosed in order to notify, or assist in the location and notification of, a family member, personal representative, or other persons responsible for the care of the patient. The amount of information disclosed to such persons should be limited to the patient's location, general condition, or death.

Logging of Disclosure

Disclosures made for notification purposes must be logged in accordance with the separate policy regarding accounting of disclosures (*See* Policy 35 – Content of Accounting of Disclosures). Disclosures made to family members who are assisting in the patient's treatment do not have to be logged.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: DISCLOSING PROTECTED HEALTH INFORMATION FOR WORKERS' COMPENSATION / EMPLOYERS

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Disclosing Protected Health Information for Workers' Compensation / Employers policy to provide teammates with guidance regarding the appropriate circumstances and procedures for the disclosure of protected health information to employers.

POLICY:

The Company may, under certain circumstances, disclose an individual's protected health information to an employer.

Disclosures of protected health information may be made to the patient's employer only in accordance with this policy.

Basic Requirements

Do not disclose the employee's health information to the employer unless the employee has provided a written authorization allowing disclosure to the employer or the employee is being evaluated, at the request of the employer, for workplace related injuries or conditions.

Authorization from Employee

Information may be disclosed to the employer if the Company has received the patient's written authorization to release the information.

Workplace-Related Evaluations

Information may be disclosed to the employer even without the patient's written authorization as long as all the following requirements are met:

A) At the request of the employer, the Company provided the patient with an evaluation relating to medical surveillance of the workplace (as required by OSHA and other state and federal agencies) or to determine whether the patient suffered a work-related illness or injury; and

B) The only information reported to the employer consists of findings concerning the patient's work-related illness or injury or a workplace-related medical surveillance; and

C) The Company obtains written certification from the employer containing the following or similar wording: "Employer certifies that it needs the disclosed health information to comply with its obligations regarding workplace and occupational safety, as set forth in 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance;" and

D) The Company provides the patient with written notice that the findings will be disclosed to the patient's employer.

Verification of Identity and Relationship

If the person requesting the information is not known to the Company, obtain and document verification of the employment relationship and the person's identity and authority to obtain information on behalf of the employer. If necessary, obtain a name and telephone number to confirm such information, or ask that the request be submitted on the employer's official letterhead. If any doubt exists, contact either the patient or the Privacy Official.

Logging of Disclosure

All disclosures to employers must be logged in accordance with the separate policy regarding accounting of disclosures (*See* Policy 35 – Content of Accounting of Disclosures).

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: DISCLOSING PROTECTED HEALTH INFORMATION FOR PUBLIC RELEASE

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Disclosing Protected Health Information for Public Release policy to provide teammates with guidance regarding the Company's procedures for disclosing protected health information for public health activities.

POLICY:

Disclosures to Public Health Authorities

Patient health information may be disclosed to a public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions. "Public health authority" means a federal, state, or local agency, or any person or entity acting under a grant of authority from such public agency that is responsible for public health matters as part of its official mandate.

Disclosures to Report Child Abuse or Neglect

Patient health information may be disclosed to a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect.

Disclosures Regarding FDA-Regulated Products and Activities

Patient health information may be disclosed to persons responsible for an FDA-regulated product or activity, for purposes related to the quality, safety, or effectiveness of the FDA-regulated product or activity. Such purposes include the following:

A) To collect or report adverse events (or similar activities 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;

B) To track FDA-regulated products;

C) To enable product recalls, repairs, or replacement, or look-back activities (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of look-back activities); or

D) To conduct post-marketing surveillance.

Communicable Diseases

To the extent allowed by state law, patient health information may be disclosed to a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition. Except in an emergency, it is preferable to notify the appropriate public health authority which will then be responsible for notifying the person who may have been exposed.

Disclosures to Employer for OSHA or Similar Reporting Purposes

Patient health information may be disclosed to the patient's employer in order to allow the employer to comply with federal or state laws, including OSHA, that require reports of work-related illnesses or injuries. Such disclosures may be made only in accordance with the Company's separate policy regarding disclosures to employers (*See* Policy 16 – Disclosing Protected Health Information for Workers' Compensation / Employers).

Minimum Necessary Disclosures

All disclosures made under this policy must be limited to the minimum amount necessary to carry out the purpose of the disclosure.

Logging of Disclosure

All disclosures made for public health activities must be logged in accordance with the separate policy regarding accounting of disclosures (*See* Policy 35 – Content of Accounting of Disclosures).

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: DISCLOSING PROTECTED HEALTH INFORMATION FOR SPECIALIZED GOVERNMENT FUNCTIONS

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Disclosing Protected Health Information for Specialized Government Functions policy to provide teammates with guidance regarding the Company's procedures for disclosing protected health information for specialized government functions.

POLICY:

Specialized Government Functions

A) The Company may use and disclose the PHI of patients who are Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, as permitted by the Armed Forces under a published notice in the Federal Register, which includes the appropriate military command authorities and the purposes for which the PHI may be used or disclosed.

B) The Company may disclose PHI to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. §401, *et seq.*) and implementing authority (e.g., Executive Order 12333).

C) The Company may disclose PHI to authorized federal officials for the provision of protective services to the President or other persons authorized by 18 U.S.C. §3056, or to foreign heads of state or other persons authorized by 22 U.S.C. §2709(a)(3), or to for the conduct of investigations authorized by 18 U.S.C. §871 and §879.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION FOR RESEARCH

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Uses and Disclosures of Protected Health Information for Research policy to outline procedures for using and disclosing protected health information for research.

POLICY:

Research

A) In general, the Company will only use or disclose PHI created for the purposes of research, with the patient's authorization. However, the Company may use or disclose PHI collected for the purposes of research without patient authorization provided that:

    (1) The Company obtains documentation that an alteration to or waiver, in whole or in part, of authorization has been approved by either an Institutional Review Board (IRB), or a privacy board.

    (2) The Company obtains from the researcher representation that use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research; no PHI is to be removed from the covered entity by the researcher in the course of the review; and the PHI for which use or access sought is necessary for the research purposes.

    (3) In the case of a deceased patient, the Company obtains from the researcher representation that the use or disclosure is sought solely for research on the PHI of the decedent, and representation that the PHI is necessary for the research purposes. The Company may request documentation of the death of the patient, from the researcher.

B) For a use or disclosure to be based on documentation of approval of a waiver, the documentation will include:

(1) A statement identifying the IRB or privacy board and the date on which the alteration or waiver of authorization was approved.

(2) A statement that the IRB or privacy board has determined that the alteration or waiver of authorization satisfies the appropriate criteria.

(3) A brief description of the PHI for which use or access has been determined to be necessary by the IRB or privacy board.

(4) A statement that the waiver of authorization has been reviewed and approved under either normal or expedited review procedures.

C) The Company will ensure that the following criteria is used in granting an approval for a waiver of authorization:

(1) The use or disclosure of PHI involves no more than minimal risk to the patients;

(2) The alteration or waiver will not adversely affect the privacy rights and the welfare of the patients;

(3) The research could not practicably be conducted without the alteration or waiver;

(4) The research could not practicably be conducted without access to and use of the PHI;

(5) The privacy risks to patients whose PHI is to be used or disclosed are reasonable in relation to the anticipated benefits, if any, to the patients, and the importance of the knowledge that may reasonably be expected to result from the research;

(6) There is an adequate plan to protect the identifiers from improper use and disclosure;

(7) There is an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers, or such retention is otherwise required by law; and

(8) There are adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of PHI would be permitted by this policy.

D) The Company will ensure that the following applies to an IRB or privacy board when reviewing and approving waivers associated with a research project:

(1) An IRB will follow the requirements of the Common Rule, including the normal review procedures (7 CFR 1c.108(b), 10 CFR 745.108(b), 14 CFR 1230.108(b), 15 CFR 27.108(b), 16 CFR 1028.108(b), 21 CFR 56.108(b), 22 CFR 225.108(b), 24 CFR 60.108(b), 28 CFR 46.108(b), 32 CFR 219.108(b), 34 CFR 97.108(b), 38 CFR 16.108(b), 40 CFR 26.108(b), 45 CFR 46.108(b), 45 CFR 690.108(b), or 49 CFR 11.108(b)) or the expedited review procedures (7 CFR 1c.110, 10 CFR 745.110, 14 CFR 1230.110, 15 CFR 27.110, 16 CFR 1028.110, 21 CFR 56.110, 22 CFR 225.110, 24 CFR 60.110, 28 CFR 46.110, 32 CFR 219.110, 34 CFR 97.110, 38 CFR 16.110, 40 CFR 26.110, 45 CFR 46.110, 45 CFR 690.110, or 49 CFR 11.110);

(2) A privacy board will review the proposed research at convened meetings at which a majority of the privacy board members are present, including at least one member who is not affiliated with the Company, not connected with any entity conducting or sponsoring the research, and any person affiliated with any such entities. The alteration or waiver of authorization will be approved by the majority of the privacy board members present at the meeting, unless the privacy board elects to use an expedited review;

(3) A privacy board may use an expedited review procedure if the research involves no more than minimal risk to the privacy of the patients who are the subject of the PHI for which use or disclosure is being sought. If the privacy board elects to use an expedited review procedure, the review and approval of the alteration or waiver of authorization may be carried out by the chair of the privacy board, or by one or more members of the privacy board as designated by the chair.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: USING AND DISCLOSING PROTECTED HEALTH INFORMATION FOR MARKETING

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Using and Disclosing Protected Health Information for Marketing policy to address the specific and limited uses of PHI for marketing purposes where a patient authorization for disclosure is not required.

POLICY:

A) In general, the Company will not use or disclose protected health information for marketing purposes without an authorization from the patient. However, the Company may use or disclose PHI to make a "marketing communication" under certain circumstances without patient authorization. This "marketing communication" is considered a function of health care operations. The Company may use or disclose PHI for the purpose of a "marketing communication" when the communication:

   (1) Occurs in a face-to-face encounter with the individual;

   (2) Concerns products or services of nominal value (e.g. distribution of calendars, pens etc.); or

   (3) Concerns the Company's or a third party's health-related products and services as long as the Company is not receiving any remuneration for making the communication.

B) If the Company uses or discloses protected health information to target the communication to patients based on their health status or condition, the Company must make a determination prior to making the communication that the product or service being marketed may be beneficial to the health of the type or class of patients targeted. In addition, the communication must explain why the patient has been targeted and how the product or service relates to the patient's health.

C) The Company must make reasonable efforts to ensure that patients who decide to opt out of receiving future marketing communications are not sent such communications.

D) The Company may disclose PHI to a business associate for purposes of marketing communications only if the business associate's function is to assist the Company with conducting the "marketing communications."

E) The Company will not sell, nor allow anyone else to sell patient's protected health information.

F) If the Company receives payment for marketing/communicating treatment options to an individual, the Company will have its Notice of Privacy Practices state that it may communicate in this way and the communication will tell patients that the Company is receiving payment in exchange for the communication and will let patients know how to opt out of further similar communications. The Company will not make opting out financially or otherwise overly burdensome for the patient.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: FUNDRAISING

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Fundraising Policy in order to ensure compliance with all applicable federal or state laws and HIPAA regulations related to all fundraising activities.

POLICY:

Fundraising is defined as a communication by or on behalf of a Covered Entity or a business associate on behalf of the Covered Entity for the purpose of raising funds for the Covered Entity, including donations, appeals, or sponsorship of events, but not royalties or remittances for sale of products. Fundraising communication is a solicitation for funds and can be in writing or oral. An acknowledgement or thank you letter for receipt of a donation or update of current development project without request for additional donation would NOT be a fundraising communication. An event invitation that includes a request for a donation to attend an event, would be a fundraising communication. This policy applies to the use or disclosure of Protected Health Information (PHI) for fundraising. *Non-PHI* sources such as purchased mailing list, alumnus or employee information, or direct contact initiated by a potential donor are *not* subject to this policy. This policy includes all fundraising activities that take place within any department of the Company or on behalf of the Company.

After obtaining a patient authorization to use PHI for fundraising activities, the following PHI is permitted:

A) Patient demographics including name, address, contact information including phone number and email address, age, gender, and date of birth;

B) Dates of service;

C) Department of service (meaning information about general department of treatment, such as cardiology or oncology, that do not indicate a more specific type of diagnosis, nature of services or treatment received by the patient);

D) Treating physician name;

E) Outcome information (such as death or other sub-optimal results and may only be used to screen or exclude patient families from receiving fundraising communications); and,

F) Health insurance status (not defined in the Privacy Rule, but interpreted to mean whether patient is insured and type of insurance).

Opt-Out Requirements

Any communication, whether verbal or written, that involves a solicitation constitutes a "fundraising" communication and must contain language describing how the individual may opt out of future solicitations. "Opt-out" requirements must be clear and conspicuous and not impose an undue burden. The Company must provide "clear and conspicuous opportunity" to the patient to opt-out of future fundraising communications. If the patient opts out, it must be treated as a revocation of any prior authorization for use or disclosure of PHI for fundraising communications. The method for a patient to opt out must not impose an undue burden or more than a nominal cost on the patient. The Company should consider offering a toll-free number, an e-mail address, a web page, or similar opt-out mechanisms that are simple, quick, and low or no cost to the patient. Requiring a patient to send a written letter opting out of fundraising communications would constitute an undue burden, although including a mailing of a pre-printed, pre-paid, business reply postcard or directing a patient to an opt-out on a web page would be permitted.

The Company may permit general opt-out for all future communications, or to a particular fundraising campaign. Once implemented, however, the Company must not send such further fundraising communications. The Company may, at its discretion, allow patients to actively opt back in to receiving fundraising communications should the patient later change their mind.

The Company may not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications.

Educational Events Co-Sponsored with a Third Party

The Company may offer educational or awareness campaigns co-sponsored by a third party (e.g., American Heart Association) or include speakers or information from such third parties. The Company, however, is prohibited from sharing PHI with the third party or permitting the third party to use a Company's patient mailing list or Permitted Fundraising PHI to send co-sponsored fundraising solicitations. The Company should not include third party fundraising information within the event's communications, e.g., invitation, brochure, or similar communication tools. At the event, the third party may invite patients to provide their contact information in writing, such as a sign-up log, that clearly identifies the third party's request to contact the patients attending the event, including the possibility that they will be contacted for the third party's own fundraising efforts. No fundraising related to the third party should occur at the event.

Documentation of Patient Authorization

A copy of the patient authorization agreeing to receive fundraising information will be given to the patient and the Company/Department will keep a copy for six (6) years in the medical record or billing record.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: PROHIBITION ON SALE OF PROTECTED HEALTH INFORMATION

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Prohibition on Sale of Protected Health Information policy to address limitations on the sale of PHI.

POLICY:

In general, the Company does not sell PHI of an individual unless it has the authorization of the individual to do so.

A) The Company will not sell PHI of an individual unless it has obtained an authorization from the affected individual.

B) The sale of PHI is a disclosure of PHI by the Company where the Company directly or indirectly receives payment from the entity receiving the PHI.

C) The sale of PHI does not include any of the following, even if the Company receives payment for the disclosures:

(1) For public health purposes;

(2) For research purposes pursuant to where the only remuneration received by the Company is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for the research purposes (provided the disclosure would meet the requirements of tracking disclosures of PHI);

(3) For treatment and payment purposes;

(4) For the sale, transfer, merger, or consolidation of all or part of the Company and for related due diligence purposes;

(5) To a business associate for activities that the business associate undertakes on behalf of the Company, if the only payment provided is by the Company to the business associate for the performance of the contracted services;

(6) To the individual to whom the PHI relates;

(7) When required by law; and

(8) For any other purpose permitted by the Company's policies and applicable laws, if the only payment is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: BUSINESS ASSOCIATES

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Business Associates policy to define the Company as a multi-entity organization and describe how its privacy policies will be applied.

POLICY:

Requirements of Disclosure

A) In dealing with business associates, the Company will allow a business associate to create or receive protected health information ("PHI") on its behalf. However, the Company will obtain satisfactory assurance from the business associate that it will appropriately safeguard the information. (Please ensure a business associate agreement has been executed and is stored in the Onit Legal Contract Management System).

B) It is not necessary to establish a business associate agreement for disclosures made by the Company to another health care provider concerning the treatment of the individual.

C) The Company will document the satisfactory assurances through a written contract or other written agreement with the business associate.

D) If the Company is aware of a pattern of activity or practice that violates the satisfactory assurances the business associate has provided to the Company, the business associate will be in noncompliance with the agreement, and the Company will make reasonable efforts to cure or end the violation. If steps to end the violation are unsuccessful, the Company will consider the feasibility of terminating the business associate agreement. If termination is not feasible, the Company may report the violation to the Secretary of U.S. Department of Health and Human Services.

Business Associate Agreement

A) The agreement must establish the permitted and required uses and disclosures of such information by the business associate. The agreement may not authorize the business associate to use or further disclose the information in a manner that would violate the Company's Privacy and Security Policies.

B) The agreement may permit the business associate to use and disclose PHI for the proper management and administration of the business associate and to carry out its legal responsibilities. The agreement may also permit the business associate to provide data aggregation services relating to the health care operations of the Company.

C) The agreement must provide that the business associate will:

(1) Not use or further disclose the information other than as permitted or required by the agreement or as required by law;

(2) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its agreement;

(3) Report to the Company any use or disclosure of the information not provided for by its agreement of which it becomes aware;

(4) Ensure that any agents, including a subcontractor, to whom it provides PHI received from, or created or received by the business associate on behalf of the Company, agrees in writing to the same restrictions and conditions that apply to the business associate with respect to such information;

(5) Make available PHI to the patient in accordance with the Company's policies;

(6) Make available PHI for amendment by the patient, and incorporate any amendments to PHI in accordance with the Company's policies;

(7) Make available the information required to provide an accounting of disclosures in accordance with the Company's policies;

(8) Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the business associate on behalf of the Company available to the Secretary for purposes of determining the Company's compliance with HIPAA;

(9) Implement protections required under the Security Rule; and

(10) Notify the Company if there has been a breach of unsecured PHI.

D) The agreement must allow for termination of the agreement if the business associate is known to be in violation of the agreement. Upon termination, if feasible, the business associate must return or destroy all PHI received from or created or received by the business associate on behalf of the Company that the business associate still maintains in any form and retain no copies of such information. If such return or destruction is not feasible, extend the protections of the agreement to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: TRACKING DISCLOSURES OF PROTECTED HEALTH INFORMATION

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Tracking Disclosures of Protected Health Information policy to provide a detailed list of disclosures of protected health information ("PHI") for each patient.

POLICY:

A log will be required for all releases excluding those for purposes of treatment, payment or healthcare operations and where a signed patient authorization is provided.

A) When a hard copy of a medical record or any PHI is copied, emailed, faxed, or released to any person or entity for purposes other than treatment, payment, or operations, the action must be entered into a log. The form "Protected Health Information Disclosure Log" (*See* attached form below) must be used to document all disclosures and will be used when the patient requests an accounting of disclosures of their information. The log must include the patient's name, date of service, date of the request, a description of the information released, number of pages, and a reason for the copy, email, or fax including the destination and/or recipient of the information or record.

B) Only those departments and individuals specifically authorized to release patient information may do so.

C) The Company will work with the Privacy Official to establish specific procedures related to copying, emailing, faxing, and releasing PHI.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

PROTECTED HEALTH INFORMATION DISCLOSURE LOG

Patient Name: _______________________ Birth Date______________

(List all disclosures made without patient authorization for public health, health oversight, research, law enforcement, disaster relief, subpoenas and court orders, or any purpose OTHER THAN for treatment, payment, internal operations, or other purposes specified in the "Protected Health Information Disclosure Log" policy.)

Who Disclosed:	**Date Disclose:**	**Disclosed to (include name and address):**	**Date of Service(s) Disclosed**	**Description of information that was disclosed and # of pages (Example – ED record, 7 pages):**	**Brief statement of the reason for disclosure:**	**How disclosed: (mail, Email, fax, etc.)**

HIPAA: RESTRICTION OF USE OR DISCLOSURE

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Restriction of Use or Disclosure policy to define a patient's right to request that a specific use or disclosure of PHI be restricted.

POLICY:

A) The Company will provide patients an opportunity to request a restriction on the use or disclosure of his/her PHI. The Company does not guarantee that it will agree to restrict the use or disclosure as requested. A restriction must be requested in writing to the Privacy Official (*See* "Request for Restriction on Uses and Disclosures of Health Information" form attached below). Working with the appropriate Office Manager or Director(s), the Privacy Official will take steps to provide or deny the restriction.

B) The Company will always agree to the patient's request to restrict disclosure if the disclosure would be for payment or operations purposes and the PHI at issue only relates to a health care item or service for which the patient (or another individual on behalf of the patient) has made complete payment upfront before services are provided.

C) When feasible, the Company will attempt to honor a patient's request to limit/restrict access to specific elements of his/her medical record.

    (1) **Marking the Record**. If the request for restrictions is accepted, mark the relevant portions of the patient's records (including billing and payment records) to protect against improper use or disclosure. Notify any of the business associates who might otherwise use or disclose the information inappropriately.

D) If the Company does agree to a request for restriction, the Company will not use or disclose the PHI unless the patient terminates the restriction, or the use or disclosure of the PHI is required for purpose of providing emergency treatment to the patient. If PHI is disclosed to another provider for emergency treatment, the Company will request that the provider not further disclose the information.

E) A restriction may be terminated by the patient in written or oral form. If the patient terminates the restriction orally, the termination must be documented by appropriate Company staff. The Company may also terminate a restriction and must notify the patient. If the Company initiates the termination of restriction, the termination is only effective with respect to PHI created or received after it has notified the patient.

F) The Company will document any restrictions, denial of restrictions, and terminations of restrictions, and will notify the patient of these actions.

G) Finally, a restriction agreed to by the Company is not effective to prevent uses or disclosures permitted for the following reasons:

(1) When required for any investigation to determine the Company's compliance;

(2) Use and disclosure for facility directories; or

(3) Uses and disclosures for which authorization or the opportunity to agree or object is not required.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

REQUEST FOR RESTRICTION ON USES AND DISCLOSURES OF HEALTH INFORMATION

1. Name of requesting individual and birth date: ________________________________
2. Date of request: __________________________
3. Describe the restriction on the Organization's uses and disclosures of your health information that you are requesting and for which *service dates*:

____

____

____

Information on Your Rights to Request a Restriction
You have the right to ask us to restrict how the Organization uses and discloses your health information for purposes of treatment, payment or health care operations (*See* Notice of Privacy Practices for more information on these types of uses and disclosures). You also have the right to ask us to restrict disclosures that we make to those family members or others involved in your care or involved in payment for your care or for notification purposes. We are *not* required to agree to your request. If we do agree, we will put it in writing and will abide by the agreement except when you require emergency treatment. If we do not agree to your request we will notify you of our decision in writing.

By submitting this form, I hereby request the Organization to restrict uses and disclosures of my health information as described above. I understand that the Organization is *not* required to agree to my request.

Name: ____________________________________

Signature: _________________________________

Date: _____________________________________

Name of Teammate Who Received This Form: ________________________

Date Form Received: ____________________________

Date Sent to Privacy Official for Approval or Denial of Restriction: ______________________

HIPAA: ALTERNATIVE / CONFIDENTIAL COMMUNICATIONS

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Alternative / Confidential Communications policy to provide guidance to teammates regarding an individual's right to request confidential communications of protected health information.

POLICY:

The Company must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the Company by alternative means or at alternative locations.

Right to Request Confidential Communications

Patients have the right to request that communications from the Company be delivered by alternative means or at alternative locations (e.g., mailing test results to an alternative location/PO Box, providing a phone call to discuss protected health information rather than mailing, etc.).

Who May Request

Only the patient or the patient's authorized representative may request a confidential communication (*See* Policy 13 – Personal Representatives regarding who qualifies as a legally authorized representative).

If the person is not known to the Company, verify and document the person's identity and authority.

Form of Request

The request must be in writing, using the form entitled "Preferred Communication Form" (*See* attached form below).

Accommodation of Request

If the request is reasonable, and if acceptable arrangements have been made for payment, the request must be accommodated. Mark the relevant portions of the patient's records (including billing and payment records) to protect against improper disclosure. Notify any of the Company's business associates who might otherwise use or disclose the information improperly.

Denial of Request

Any decision to deny the request shall be made by the Privacy Official, who must document why the request was found to be unreasonable.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

Envision HEALTHCARE

PREFERRED COMMUNICATIONS FORM

Name of Patient: ______________________________ Date of Request: ________________________

I request that all communications from the Company be delivered to me by the following alternate means or at the following alternate address or phone number.

____

____

____

____

<u>Acknowledgement and Agreement</u>. I understand and agree that if this request could limit the Center's ability to collect payment, I will be responsible for paying the bill in full, and that my failure to pay within 90 days will constitute my agreement that the Company may contact me at any other known address or phone number.

SIGNED: ____________________________ Date: ___________________________

Print name: ___________________________ Phone No: ________________________

Address: ______________________________

____

Relation to patient: ______________________

For internal use only:

Date request received: ___________________ Received by: ____________

How was identity verified? _________________________ Copy made: Yes ☐ No ☐

How was authority verified? ________________________ Copy made: Yes ☐ No ☐

Date Sent to Privacy Official to approve: _______________

Privacy Official Approved: Approved: Yes _______ No _______

HIPAA: REQUEST AND DOCUMENTATION FOR ACCESS

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Request and Documentation for Access policy to identify the patient's right to access his or her medical record.

POLICY:

A) Each patient has a right of access to inspect and obtain a copy of PHI about the patient in a designated record set for as long as the PHI is maintained in the designated record set, except for:

   (1) Psychotherapy notes (defined as notes prepared by a mental health professional to document or analyze private conversations with the patient);

   (2) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and

   (3) PHI maintained by the Company that is:

      (a) Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. §263a, to the extent the provision of access to the patient would be prohibited by law (laboratory results subject to disclosure limitations under CLIA) or Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 CFR §493.3(a)(2).

      (b) Information obtained, under promise of confidentiality, from someone other than a health care provider.

      (c) Information requested by a parent regarding a minor patient, if the minor alone sought and consented to the treatment and the treating physician believes it would be in the minor's best interest to maintain the minor patient's privacy.

(d) Designated record set includes the patient's clinical records, payment and insurance records, and any other collection of health information maintained and used by the Company to make decisions about the patient. This does **NOT** include information used or created to conduct UR/QA activities, to obtain legal advice, or for other internal operations of the Company.

B) Upon written request of the patient, the Company will provide the patient with access to or a copy of his/her medical record, in whole or in part, unless it meets one of the exceptions above. In addition, the Company will not provide copies of information, where applicable law would prohibit the Company from disclosing the information to the patient, or under circumstances that would jeopardize the safety of the patient or others (*See* Policy 28 - Denial of Request for Access regarding the specifics of the circumstances allowing for denial).

C) If the patient requests specific information not contained in the medical record, but the department knows where the requested information is maintained, the patient will be informed where to direct the request for access.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: DENIAL OF REQUEST FOR ACCESS

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Denial of Request for Access policy to define the Company's reasons for denying a patient's request to access his/her medical record.

POLICY:

A) The Company may deny a patient access without providing the patient an opportunity for review, in the following circumstances:

(1) The PHI is exempted from the right of access by Policy 30 - Request and Documentation for Access.

(2) If acting under the direction of a correctional institution, the Company may deny, in whole or in part, an inmate's request to obtain a copy of PHI, if obtaining such copy would jeopardize the health, safety, security, custody, or rehabilitation of the patient or of other inmates, or the safety of any Official, employee, or other person responsible for the inmate.

(3) A patient's access to PHI created or obtained in the course of research may be temporarily suspended for as long as the research is in progress, provided that the patient has agreed to the denial of access when consenting to participate in the research, and the Company has informed the patient that the right of access will be reinstated upon completion of the research.

(4) A patient's access to PHI that is contained in records that are subject to the Privacy Act, 5 U.S.C. §552a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.

(5) A patient's access may be denied if the PHI was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

(6) Health records include the patient's clinical records, payment and insurance records, and any other collection of health information maintained and used by the Company to make decisions about the patient. This does **NOT** include information used or created to conduct UR/QA activities, to obtain legal advice, or for other internal operations of the Company.

B) The Company may deny a patient access, provided that the patient is given a right to have such denials reviewed, in the following circumstances:

(1) A licensed health care professional has determined that the access requested is reasonably likely to endanger the life or physical safety of the patient or another person;

(2) The PHI makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined that the access requested is reasonably likely to cause substantial harm to such other person; or

(3) The request for access is made by the patient's personal representative and a licensed health care professional has determined that the provision of access to such personal representative is reasonably likely to cause substantial harm to the patient or another person.

C) If access is denied on a ground permitted under section (B) of this policy, the patient has the right to have the denial reviewed by a licensed health care professional. The Company must designate a licensed health care professional, who was not directly involved in the denial, to review the decision to deny access. The Company must promptly refer a request for review to such designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested. The covered entity must promptly provide written notice to the individual of the determination of the designated reviewing official, and take other action as required to carry out the designated reviewing official's determination.

D) If the Company denies access, in whole or in part, to PHI, the Company will, to the extent possible, give the patient access to any other PHI requested after excluding the PHI as to which the Company has a ground to deny access. In addition, the Company will provide a timely, written denial to the patient, in accordance with Policy 29 - Provision of Access, sections (B) and (C). The denial must be in plain language and contain:

(1) The basis for the denial;

(2) If applicable, a statement of the patient's review rights including a description of how the patient may exercise such review rights; and

(3) A description of how the patient may complain to the Company or to the Secretary of the U.S. Department of Health and Human Services for failure to comply with the patient's request. The description must include the name, or title, and telephone number of a contact person or office related to privacy and security.

E) If the Company does not maintain the PHI that is the subject of the patient's request for access, and the Company knows where the requested information is maintained, the Company will inform the patient where to direct the request for access.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: PROVISION OF ACCESS

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Provision of Access policy to identify the Company's requirements for processing a request for access to a patient's medical record.

POLICY:

A) A patient must submit a request for access in writing to the Company's Privacy Official (*See* form entitled "Patient Request to Inspect Health Information," attached below).

B) The Company will act on a request for access to records that are not in an electronic format no later than **thirty (30) days** after receipt of the request as follows.

(1) If the request is not denied, the Company will inform the patient of the acceptance of the request and provide the access requested.

(2) If the request is denied, in whole or in part, the Company will provide the patient with a written denial, in accordance with Policy 28 – Denial of Request for Access.

C) If the Company is unable to take an action within the time required, the Company may extend the time for such actions by no more than **thirty (30) days**, provided that:

(1) The Company, within the time limit set by sections (B) and (C) of this policy, as applicable, provides the patient with a written statement of the reasons for the delay and the date by which the Company will complete its action on the request; and

(2) The Company may have only one such extension of time for action on a request for access.

D) If the Company provides a patient with access, in whole or in part, to PHI, the Company must comply with the following requirements.

(1) The Company will provide the access requested by patients, including inspection or obtaining a copy, or both, of the PHI about them in designated record sets. If the same PHI that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the Company will only produce the PHI once in response to a request for access.

(2) The Company will provide the patient with access to the PHI in the form or format requested by the patient, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by the Company and the patient.

(3) The Company may provide the patient with a summary of the PHI requested, in lieu of providing access to the PHI, or may provide an explanation of the PHI to which access has been provided if the patient agrees in advance to such summary or explanation and to any the fees that may be imposed.

(4) The Company will provide the access as requested by the patient in a timely manner, including arranging with the patient for a convenient time and place to inspect or obtain a copy of the PHI, or mailing the copy of the PHI at the patient's request. The Company may discuss the scope, format, and other aspects of the request for access with the patient, as necessary, to facilitate the timely provision of access.

(5) If the patient requests a copy of the PHI or agrees to a summary or explanation of such information, the Company may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:

(a) Copying, including the cost of supplies for and labor of copying, the PHI requested by the patient;

(b) Postage, when the patient has requested the copy or the summary or explanation, be mailed; and

(c) Preparing an explanation or summary of the PHI, if agreed to by the patient.

E) The Company will document the designated record sets that are subject to access by patients and the titles of the persons or offices responsible for receiving and processing requests for access by patients. All documentation, including requests and denials, will be retained for six (6) years from the date of document creation or the date it last was in effect, whichever is last.

F) If the PHI requested is in an electronic format, the Company will provide the patient with the PHI in an electronic format requested by the patient, if able to do so, or in a readable electronic format that the patient and the Company agree to.

G) If the patient requests that the Company transmit a copy of the PHI requested to a third party, the Company will provide a copy of the PHI to that third party provided that the patient's request is:

(1) In writing;

(2) Signed by the individual;

(3) Clearly identifies the designated person and where to send the copy of the information.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

PATIENT REQUEST TO INSPECT HEALTH INFORMATION

(This request must be completed and submitted to the Center along with verification of your identity. If you are not the patient, you must also provide proof of your relation to the patient or other legal authority to obtain access to the patient's health information.)

I, ____, hereby request that I be allowed to inspect and/or obtain a copy of health information regarding the following patient:

Patient Name: ____________________________________ Date of Birth:____________
Address: ____ Phone: _________________
____

4. **I wish to** (check one or more of the following):

   ☐ Personally inspect the patient's health records at no charge, at a mutually convenient time.

   ☐ Obtain a copy of the patient's health records. I understand that there is a copying charge of $__________ per page and that I may be required to pay the copying charge, plus any costs of postage, before the copies will be released to me.

   ☐ Obtain a summary of information in the patient's health records, at a charge of $________.

5. **The information to be inspected and/or copied includes only those items checked below:**

   ☐ Billing and payment information (*If you only need information regarding certain dates or types of treatment, please describe below.*)

   ____
   ____
   ____

   ☐ Medical record (*If you only need information regarding certain dates or types of treatment, please describe below.*)

   ____
   ____
   ____

   ☐ A summary of information in the medical record (*If you only need information regarding certain dates or types of treatment, please describe below.*)

   ____
   ____
   ____

6. **I certify that I am** (check whichever applies)**:**

☐ the patient, and the identification that I have provided is true and correct.

☐ the patient's authorized representative, and that the identification and proof of authority that I have provided are true and correct. My relationship to the patient is that of ____________________________________.

Signed this _____ day of ____________________, 20___.

Signed: ____________________________________

Print name: _________________________________

Address: ___________________________________

____

Witness: ____________________________________

Print name: _________________________________

Date: ______________________________________

- -

For Office Use Only:

Date request received: __________________

How was identity verified? ______________________________ Copy made? ☐ Yes ☐ No

How was authority verified? _____________________________ Copy made? ☐ Yes ☐ No

Information/Copies made available by: ________________________________ Date: _______

HIPAA: REQUEST AND DOCUMENTATION FOR AMENDMENT

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Request and Documentation for Amendment policy to identify the patient's right to amend his/her medical record.

POLICY:

A patient has the right to have PHI or a record about the patient in a designated record set amended for as long as the PHI is maintained in the designated record set (*See* form "Patient Request for Amendment of Health Information" attached below).

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

Envision HEALTHCARE

PATIENT REQUEST FOR AMENDMENT OF HEALTH INFORMATION

Patient Name: ____

Birth Date: ____

Patient Account Number: ______________________________________

Date of Service: ____

Patient Address: ____

____

Date of entry to be amended: ___________________________________

Type of entry to be amended**:** __________________________________

Please explain how the entry is incorrect or incomplete. What should the entry say to be more accurate or complete?

____

____

____

____

Signature of Patient or Legal Representative Date

____

Relationship of Legal Representative

For Healthcare Organization Use Only:

Date Received: ____________________ Amendment has been: □ Accepted □ Denied

If denied, check reason for denial:

- □ PHI was not created by this organization
- □ PHI is not available to the patient for inspection as required by federal law (e.g. psychotherapy notes)
- □ PHI is not part of patient's designated record set
- □ PHI is accurate and complete

HIPAA: DENIAL OF AMENDMENT

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Denial of Amendment policy to define the Company's reasons for denying a patient's request to amend his/her medical record.

POLICY:

A) The Company may deny a patient's request for amendment if it determines that the PHI or record that is the subject of the request:

(1) Was not created by the Company, unless the patient provides a reasonable basis to believe that the originator of PHI is no longer available to act on the requested amendment;

(2) Is not part of the designated record set;

(3) Would not be available for inspection under Policy 27 - Request and Documentation for Access; or

(4) Is accurate and complete.

B) If the Company denies a patient's request for amendment, the Company must provide the patient with a written denial within sixty (60) days of the date the request is received. The Privacy Official will provide the patient with the written denial. The denial must be written in plain language and contain:

(1) The basis for the denial;

(2) The patient's right to submit a written statement disagreeing with the denial and how the patient may file such a statement;

(3) A statement that, if the patient does not submit a statement of disagreement, the patient may request that the Company provide the patient's request for

amendment and the denial with any future disclosures of the PHI that is the subject of the amendment; and

(4) A description of how the patient may complain to the Company or to the Secretary of the U.S. Department of Health and Human Services for failure to comply with the patient's request. The description must include the name or title and telephone number of a contact person or office related to privacy and security.

C) If the Company is unable to provide a written denial within the time required, the Privacy Official may extend the time by no more than thirty (30) days, provided that the Privacy Official, within sixty (60) days of receipt of a request, provides the patient with a written statement of the reasons for the delay and the date by which the Company will complete its action. The Company may have only one such extension of time for action on a request for amendment.

D) The Company permits the patient to submit to the Privacy Official a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The Company may reasonably limit the length of a statement of disagreement.

E) The Company may prepare a written rebuttal to the patient's statement of disagreement. Whenever such a rebuttal is prepared, the Privacy Official will provide a copy to the patient who submitted the statement of disagreement.

F) The Company will, as appropriate, identify the record or PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link the patient's request for an amendment, the Company's denial of the request, the patient's statement of disagreement, if any, and the Company's rebuttal, if any, to the designated record set (document or transaction).

G) If a statement of disagreement has been submitted by the patient, the Company must include the material appended or, at the election of the Company, an accurate summary of any such information, with any subsequent disclosure of the PHI to which the disagreement relates.

H) If the patient has not submitted a written statement of disagreement, the Company will, upon request of the patient in writing, include the request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the PHI. When a subsequent disclosure is made using a standard transaction (as defined by the HIPAA Transaction Rules) that does not permit the additional material to be included with the disclosure, the Company may separately transmit the request for amendment and its denial, or summary of such information, to the recipient of the standard transaction.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: PROVISION OF AMENDMENT

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Provision of Amendment policy to identify the Company's requirements for processing a request for amending a patient's medical record.

POLICY:

A) If the Company grants the requested amendment, the Company must act on the patient's request for an amendment no later than sixty (60) days after receipt of such a request.

B) If the Company is unable to take an action on the patient's request within the time required, the Privacy Official may extend the time by no more than thirty (30) days, provided that the Privacy Official, within sixty (60) days of receipt of a request, provides the patient with a written statement of the reasons for the delay and the date by which the Company will complete its action on the request. The Company may have only one such extension of time for action on a request for amendment.

C) If the Company grants the requested amendment, the Company will make the appropriate amendment by identifying the records in the designated record set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment. The Company will inform the patient that the amendment is accepted. With the patient's agreement, the Company will notify the relevant persons with which the amendment needs to be shared. Relevant persons include persons identified by the patient as having received PHI about the patient and needing the amendment, and persons, including business associates, that the Company knows have the PHI that is the subject of the amendment and that may have relied, or could rely, on such information to the detriment of the patient.

D) If informed by another health care provider or another agency of an amendment to a patient's PHI, the Company will amend the PHI in designated record sets.

E) The Company will document the titles of the persons or offices responsible for receiving and processing requests for amendment by patients. All documentation, including requests and denials, will be retained for six (6) years from the date of document creation or the date it last was in effect, whichever is last.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: REQUEST AND DOCUMENTATION OF ACCOUNTING OF DISCLOSURES

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Request and Documentation of Accounting of Disclosures policy to identify the patient's right to request an accounting of disclosures of his/her medical record.

POLICY:

A) A patient has the right to receive an accounting of disclosures of PHI made by the Company in the six (6) years prior to the date on which the accounting is requested, except for disclosures:

   (1) To carry out treatment, payment, and health care operations;

   (2) To patients of PHI about them;

   (3) For the facility's directory or to persons involved in the patient's care or other notification purposes;

   (4) For national security or intelligence purposes; or

   (5) To correctional institutions or law enforcement officials.

B) The Company will temporarily suspend a patient's right to receive an accounting of disclosures to a health oversight agency or law enforcement official for the time specified by such agency or official. Such agency or official must provide the Company with a written or verbal statement that such an accounting to the patient would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required. If the agency or official statement is made orally, the Company will:

   (1) Document the statement, including the identity of the agency or official making the statement;

(2) Temporarily suspend the patient's right to an accounting of disclosures subject to the statement; and

(3) Limit the temporary suspension to no longer than thirty (30) days from the date of the oral statement, unless a written statement is submitted during that time.

C) A patient may request an accounting of disclosures for a period of time less than six (6) years from the date of the request.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: PROVISION OF ACCOUNTING OF DISCLOSURES

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Provision of Accounting of Disclosures policy to identify the Company's requirements for processing a request for an accounting of disclosures of a patient's medical record.

POLICY:

A) The Company will act on the patient's request for an accounting, no later than sixty (60) days after receipt of such a request. The Company will provide the patient with the accounting requested, or if unable to provide the accounting within the time required, the Privacy Official may extend the time to provide the accounting by no more than thirty (30) days, provided that the Company, within sixty (60) days after receipt of a request, provides the patient with a written statement of the reasons for the delay and the date by which the Company will provide the accounting. The Company may have only one such extension of time for action on a request for an accounting.

B) The Company will provide the first accounting to a patient in any 12-month period without charge. The Company may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same patient within the 12-month period. The Company will inform the patient in advance of the fee and provide the patient with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

C) The Company will document the titles of the persons or offices responsible for receiving and processing requests for an accounting by patients. All documentation, including requests for accounting, denials, and the written accounting, provided to the patient will be retained for six (6) years from the date of document creation or the date it last was in effect, whichever is last.

D) If the Company determines that it must exclude PHI from an accounting of disclosures for any of the reasons described in Policy 33 - Requests and Documentation of Accounting Disclosures, the Company will provide a timely, written explanation to the patient. The explanation will be in plain language and contain:

(1) The basis for the exclusion; and

(2) A description of how the patient may complain to the Company or to the Secretary of the U.S. Department of Health and Human Services for failure to comply with the patient's request, in whole or in part. The description must include the name or title and telephone number of a contact person or office related to privacy and security.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: CONTENT OF ACCOUNTING OF DISCLOSURES

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Content of Accounting of Disclosures policy to identify the content of an accounting of disclosures of a medical record.

POLICY:

A) When providing a patient with an accounting, the accounting must include disclosures of PHI that occurred during the six (6) years (or such shorter time period at the request of the patient) prior to the date of the request for the accounting, including disclosures to or by business associates of the Company.

B) The accounting must include for each disclosure:

   (1) The date of the disclosure;

   (2) The name of the entity or person who received the PHI and, if known, the address of such entity or person;

   (3) A brief description of the PHI disclosed; and

   (4) A brief statement of the reason of the disclosure that reasonably informs the patient of the basis for the disclosure.

C) If, during the period covered by the accounting, the Company has made multiple disclosures of PHI to the same person or entity for a single purpose, or pursuant to a single authorization for use or disclosure, the accounting may provide:

   (1) The information required for the first disclosure during the accounting period;

   (2) The frequency, periodicity, or number of the disclosures made during the accounting period; and

(3) The date of the last such disclosure during the accounting period.

D) List of Exempt Disclosures (Accounting does not have to include disclosures made for below purposes):

(1) Treatment, payment, or healthcare operations;

(2) Disclosures to the patient or the patient's personal representative;

(3) Disclosures authorized by the patient or the patient's representative;

(4) To notify family members or to assist family and other persons involved in the patient's care;

(5) For national security intelligence;

(6) To correctional institutions or law enforcement authorities that have custody of the patient;

(7) Disclosures involving de-identified information.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: GENERAL REQUIREMENTS FOR DISCLOSURE OR RELEASE OF INFORMATION

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this General Requirements for Disclosure or Release of Information policy to define the process requirements for disclosing PHI.

POLICY:

The process of disclosure will vary based on the content of the information and the circumstances surrounding the disclosure.

A) In general, the Company will disclose a patient's PHI to any person, entity, or company only:

   (1) After verification that the disclosure is authorized by the treatment, payment, or operations definitions of the Privacy Regulations;

   (2) The disclosure is to a bona fide Business Associate;

   (3) The disclosure is to the patient him/herself; or

   (4) A valid authorization has been received.

B) The department may use or disclose PHI without prior written consent under the following circumstances:

   (1) If the Company has an indirect treatment relationship with the patient;

   (2) In emergency treatment situations;

   (3) If required by law; or

(4) If the patient's consent to receive treatment is clearly inferred from the circumstances.

C) The Company will not disclose an entire medical record except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request.

D) The Company will release information that was received or created outside the process of providing treatment, payment, or health care operations, only with direct authorization from the patient. When releasing information based on a patient authorization, the department will only disclose information consistent with terms of the authorization.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: VERIFICATION OF PERSON(S) REQUESTING PHI

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to “teammate” or “teammates” include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates (“Envision” or “the Company”) has adopted this Verification of Person(s) Requesting PHI policy to establish that the Company will not release information to unknown individuals.

POLICY:

For each disclosure of PHI to an individual or organization that is not known by the Company, the Company will take reasonable steps to verify the identity and authority of the individual or organization to which PHI is disclosed.

Requests made in person

Reasonable steps may include a request to see positive identification of a person (e.g., driver’s license or other government issued photo identification).

Requests made over the telephone

Reasonable steps may include verification of identity thru information that would only be known to an authentic personal representative (e.g., social security number – last four digits, date of birth, telephone number, maiden name, spouse’s name).

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company’s Ethics & Compliance Program.

HIPAA: AUTHORIZATION REQUIREMENTS

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Authorization Requirements policy to outline the Company's requirements for patient authorization related to the use and disclosure of PHI.

POLICY:

General Requirements

Except for the uses and disclosure identified in Policy 25 – Restriction of Use or Disclosure, the Company will not use or disclose PHI that was received or created outside the process of providing treatment, payment, or health care operations, without an authorization from the patient. When the Company obtains or receives a valid authorization for its use or disclosure of PHI, such use or disclosure must be consistent with such authorization.

A) The Company will not obtain a patient's authorization to disclose PHI when required by law, as part of health oversight activities, for the purpose of identifying a deceased person, or when a waiver is granted for the purposes of a research project.

Defective Authorizations

A) An authorization is not valid, if the document submitted has any of the following defects:

   (1) The expiration date has passed, or the expiration event is known by the covered entity to have occurred;

   (2) The authorization has not been filled out completely;

   (3) The authorization has been revoked;

   (4) The authorization does not contain all the required elements as defined in this policy;

(5) Any material information in the authorization is known to be false.

Conditioning of Authorizations

A) The Company will not condition treatment on the provision of an authorization, except that the Company may condition the provision of "research-related" treatment on provision of an authorization.

B) The Company may also condition the provision of health care that is solely for the purpose of creating PHI for disclosure to a third party. For example, the Company may have a contract with an employer to provide fitness-for-duty exams, or a contract with a life-insurer to provide pre-enrollment physicals for applicants. In each of these cases, the Company would condition the health care services on provision of an authorization.

Revocation of Authorizations

A) The Company will allow a patient to revoke an authorization at any time, provided that the revocation is in writing, except to the extent that the Company has taken action in reliance thereon.

Documentation Requirements

A) The Company will retain any signed authorization and related documentation for six (6) years from the signed date of the authorization.

B) The Company will provide the patient with a copy of the authorization.

C) The authorization must be written in plain language.

Core Elements and Requirements

A) The authorization must contain the following elements:

(1) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;

(2) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;

(3) The name or other specific identification of the person(s), or class of persons, to whom the Company may make the requested use or disclosure;

(4) An expiration date or an expiration event that relates to the patient or the purpose of the use or disclosure;

(5) A statement of the patient's right to revoke the authorization in writing and the exceptions to the right to revoke, together with a description of how the patient may revoke the authorization;

(6) A statement that information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and no longer be protected by this rule;

(7) Signature of the patient and date; and

(8) If the authorization is signed by a personal representative of the patient, a description of such representative's authority to act for the patient.

See "Authorization to Release Health Information," form attached below.

B) If the Company requests the authorization for its own uses, or for the use or disclosure by others, the following apply:

(1) A statement that the Company will not condition treatment on the patient's providing authorization for the requested use or disclosure;

(2) A description of each purpose of the requested use or disclosure;

(3) A statement that the patient may inspect or copy the protected health information to be used or disclosed, and refuse to sign the authorization;

(4) If use or disclosure of the requested information will result in direct or indirect remuneration to the Company from a third party, a statement that such remuneration will result; and

(5) A statement that the patient may refuse to sign the authorization.

Authorization for Research that Includes Treatment

A) If the Company creates PHI for the purpose, in whole or in part, of research that includes treatment of patients, the Company will obtain an authorization for the use or disclosure of such information. The authorization will contain:

(1) A description of the extent to which such PHI will be used or disclosed to carry out treatment, payment, or health care operations;

(2) A description of any PHI that will not be used or disclosed for any purposes permitted by law, provided that the Company will not limit its right to make a use or disclosure that is required by law or permitted by law to mitigate a serious and imminent threat to public health or safety; and

(3) The authorization will refer to any patient consent and to the Notice of Privacy Practices, as applicable, and will state that the statements made pursuant to this section are binding.

(4) An authorization under this paragraph may be in the same document as a consent to participate in the research, a consent to use or disclose PHI to carry out treatment, payment, or health care operations, or a Notice of Privacy Practices.

Compound Authorizations

A) The Company will not combine any authorizations for use or disclosure with a consent for treatment or payment or with an informed consent to participate in research.

B) The Company may combine an authorization for use or disclosure of PHI and another document to create a compound authorization as follows:

(1) An authorization created for research that includes treatment of the patient may be combined with a consent for use or disclosure, another research consent, or a Notice of Privacy Practices;

(2) An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes; and

(3) An authorization, other than an authorization for disclosure of psychotherapy notes, may be combined with any other authorization, except when treatment is conditioned on the provision of one of the authorizations.

(4) An authorization for disclosure of PHI for a research study can be combined with any other type of written permission for the same or another research study, with an authorization for the creation or maintenance of a research database or repository or with a consent to participate in research.

C) If authorizations are combined as described in this policy, each authorization must be visually and organizationally separate from other content within the document, and it must be separately signed and dated.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

Envision HEALTHCARE

AUTHORIZATION TO RELEASE HEALTH INFORMATION

Patient Name:

Patient Address:

Date of Birth (mm/dd/yy): Patient's Phone:

Other Identifier (Last 4 digits of Social Security #):

I AUTHORIZE ________________________________

TO DISCLOSE MY HEALTH INFORMATION TO: ________________________

Name of person or organization:

To the Attention of:

Street Address of Entity:

City: State: Zip: Phone or Email of Recipient:

Information to be Disclosed. The information to be disclosed includes only those items checked below, with respect to services provided on or around __________________________ *(insert dates)*:

☐ The following medical records:

❑ Discharge summary	❑ Progress notes
❑ Lab results	❑ Photographs, videotapes, or other images
❑ History and physical exam	❑ Mental or behavioral health records
❑ Consultation reports	❑ Psychotherapy notes
❑ X-ray reports	❑ Genetic test results
❑ HIV/AIDS test results and treatment	❑ Entire medical record
❑ Alcohol and drug treatment records	❑ Summary of treatment
❑ Operative record	❑ Other (specify):

☐ The following billing and payment information:

____

____

☐ Other information: ____

____

REASON FOR REQUESTED USE OR DISCLOSURE:
TO BE READ AND SIGNED BY PATIENT OR LEGAL REPRESENTATIVE:

I understand the following:

a. I may revoke this authorization at any time by providing written notice.
b. I may not be able to revoke this authorization if the company has already taken action utilizing this authorization or if the authorization was obtained as a condition of obtaining insurance coverage.
c. I understand that I may refuse to sign this Authorization and that the company will not condition treatment on whether I sign this Authorization.
d. I am signing this authorization freely and no one has pressured me to sign this authorization.
e. The information disclosed in this authorization may be subject to re-disclosure by the receiving party and no longer protected by federal law.
f. I acknowledge that I have had an opportunity to review this authorization and understand the intent and the use.
g. Expiration: I understand that unless I revoke the authorization earlier, this authorization will automatically expire one (1) calendar year after the date this authorization is signed.

Patient Signature:		Date:
Signature of Patient's Representative:	Relationship:	Date:

FOR OFFICE USE ONLY:

Event or Date Upon Which Authorization Will Expire:

If no date is specified, this authorization will expire within 1 year of the date above.

HIPAA: SPECIAL HANDLING OF RESTRICTED CONFIDENTIAL INFORMATION

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Special Handling of Restricted Confidential Information policy to establish guidelines for disclosing the most sensitive of protected health information. This use and disclosure of this information is typically highly regulated by State and Federal regulations. Accordingly, this information may not be handled or released in the same manner as other PHI.

POLICY:

Disclosure of Psychotherapy Notes

A) In general, the Company will obtain a patient authorization for the release of psychotherapy notes. However, the department may rely upon the patient's consent for use or disclosure for the following:

(1) For the provider, individual originator of the psychotherapy notes, to provide treatment;

(2) For use in supervised training programs; or

(3) For defending a legal action or other proceeding brought by the individual; and

(4) The Company will not obtain a patient's authorization to disclose psychotherapy notes when required by law, as part of health oversight activities, for the purpose of identifying a deceased person, or when a waiver is granted for the purposes of a research project.

Copying and Faxing

A) The following types of medical information are typically protected by federal and/or state statute and may NOT be photocopied, emailed, mailed, or faxed without specific patient authorization or when required by law:

(1) Psychotherapy (from records of treatment by a psychiatrist, licensed psychologist, or psychiatric clinical nurse specialist);

(2) Other professional services of a licensed psychologist;

(3) Social Work Counseling/Therapy;

(4) Domestic Violence Victims' Counseling;

(5) Sexual Assault Counseling;

(6) Records Pertaining to Sexually-Transmitted Diseases;

(7) HIV Test Results (patient authorization required for EACH release request.); and

(8) Alcohol and Drug Abuse Records Protected by Federal Confidentiality Rules (42 CFR Part 2).

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: RESPONSIBILITIES

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Responsibilities policy to provide a mission statement for the Company in addressing patient privacy and information security issues.

POLICY:

It is the role of all teammates to maintain the confidentiality and security of protected health information in order to ensure the patient's right to privacy. Guidance, direction, and authority for privacy and security activities is the responsibility of the Executive Management team and as delegated by this policy to the Enterprise Privacy Official and the Enterprise Security Official.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: ORGANIZATIONAL STRUCTURE

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Organizational Structure policy to establish the internal Company responsibilities for the oversight of privacy issues.

POLICY:

The Company has established and maintains formal privacy and security compliance programs and management structure responsible for monitoring and maintaining security and confidentiality standards throughout the organization. The Privacy and Security Officials will oversee the daily management of program activities, and will work closely with the Company's departmental directors, administrators, and other management staff. The Privacy Official and Security Official will report, as necessary, at the Compliance Integrity Committee meetings. In this way, the Company has provided a single point of contact responsible for the management of privacy and security issues.

The Company has designated the Privacy and Security Officials as the officials responsible for the development and implementation of the security/confidentiality policies and procedures. The Privacy Official will report significant violations and compiled data to the Compliance Integrity Committee. The Privacy and Security Officials will coordinate with appropriate departmental managers to ensure proper implementation of security measures, training programs, and privacy rules.

The Privacy Official and/or Security Official will:

A) Guide the development of information privacy objectives and policies;

B) Develop implementation plans and propose budgets to support objectives and policies;

C) Guide the implementation of information privacy objectives and policies;

D) Determine the methodology and procedures for accomplishing the goals of the information privacy regulations;

E) Manage privacy incidents policies and procedures;

F) Direct training and awareness programs;

G) Oversee on-going privacy monitoring processes;

H) Research and understand privacy/confidentiality related regulatory requirements such as HIPAA and state privacy regulations in tandem with the Legal Department;

I) Research and understand privacy-related technologies;

J) Execute directives of senior management and the Compliance Integrity Committee related to privacy and confidentiality of patient information; and

K) Inform senior management and the Compliance Integrity Committee on privacy issues and make recommendations.

The Compliance and Integrity Committee will meet at least quarterly to:

A) Review the current status of the Company's privacy and security compliance;

B) Review and monitor privacy and security incidents within the Company;

C) Approve and review privacy projects;

D) Approve new or modified privacy and security policies; and

E) Perform other necessary high-level information security management activities.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: MANAGEMENT ROLE

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Management Role policy to identify the responsibilities of the Company's directors and managers with regard to ensuring privacy.

POLICY:

Directors and Managers are responsible for implementing the prescribed security and privacy processes in a fashion that is consistent with the criticality, value, and sensitivity of the information being handled.

Managers are also responsible for documenting patient complaints with regard to privacy, escalating said complaints to the Privacy Official for tracking and trending purposes, and for administering corrective actions in accordance with People & Culture disciplinary policies for employees known to be in violation of the Company's privacy rules.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: OTHER PRIVACY & SECURITY ROLES

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Other Privacy & Security Roles policy to define a broader range of privacy and security responsibilities. Both the security and privacy of PHI is an organization-wide responsibility and must be guarded by all members of the workforce.

POLICY:

A) All outside consultants, contractors, and temporary workers must be subject to the same information security and privacy requirements as Company employees. This includes, but is not limited to physicians, students, consultants, and out-sourced employees.

B) Any outside visitor to the Company shall be challenged regarding his or her presence in areas deemed restricted or proximate to PHI.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: ADHERING TO POLICIES AND PROCEDURES

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Adhering to Policies and Procedures policy to communicate that all teammates are required to comply with privacy and security policies.

POLICY:

A) The Company has implemented policies and procedures, with respect to PHI, designed to comply with the standards, implementation specifications, and other requirements of the Standards for Privacy of Individually Identifiable Health Information.

B) The Company reserves the right to revise its policies and procedures. When changes are made, the Company will promptly notify and educate staff on these changes. Company employees are responsible for understanding and complying with these policies and procedures. Violations of these policies and procedures will not be tolerated and may subject the employee to disciplinary actions up to and including termination of employment.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: COMPLAINTS / INCIDENT REPORTING

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Complaints / Incident Reporting policy to identify a process for filing complaints and reporting violations related to a patient's right to privacy and the Company's privacy and security policies.

POLICY:

A) A person who believes the Company is not complying with the applicable requirements of the privacy or security processes may file a complaint with the Privacy Official and/or the Secretary of U.S. Department of Health and Human Services.

B) Complaints made to the Secretary must meet the following requirements:

(1) A complaint must be filed in writing, either on paper or electronically.

(2) A complaint must name the entity that is the subject of the complaint and describe the acts or omissions believed to be in violation of the applicable standards, requirements, and implementation specifications of the privacy or security regulations.

(3) A complaint to the Secretary must be filed within one hundred eighty (180) days of when the complainant became aware, or should have known, that the act or omission complained about in the communication occurred, unless this time limit is waived by the Secretary.

C) The Company acknowledges that the Secretary is empowered to and "may investigate" any complaints. Accordingly, the Company will cooperate with any investigation or compliance review. The Company will keep records including pertinent policies, procedures, or practices and of the circumstances regarding any alleged violation. The Company will submit compliance reports or corrective action plans, in a timely manner as requested by the Secretary.

D) The Company's Privacy Official, in cooperation with appropriate department managers, will investigate any alleged violation of the Company's privacy policies, and take appropriate action to remedy the violation and initiate a personnel action as appropriate in partnership with the People & Culture Department.

E) The Company will include contact information for filing a complaint in its Notice of Privacy Practices. The contact information will include the name, title, and telephone number of the Company's Privacy Official.

F) Teammates must report any known or suspected violation of privacy or security policies, or any known or suspected breach of security to their department managers immediately. Department managers will report the violation or breach to the Privacy Official or Security Official. All reports should be communicated maintaining strict confidentiality. Teammates may utilize the "Helpline" as a means to report a violation or breach (toll-free 877-835-5267).

G) The Privacy Official will initiate a formal problem management process to record the problems, to reduce their incidence, and to prevent their recurrence. Consistent with Compliance Investigations policy and procedure, an investigation shall commence within a reasonable time frame after reported. Aggregate data related to violations reported will be presented to the Compliance Integrity Committee.

H) To ensure a quick, effective, and orderly response to incidents, the Company must maintain procedures for handling privacy violations and security incidents. Key individuals responsible for assisting in the investigation and correction of security incidents are clearly defined in the policies of the Information Technology Department under the leadership of the Security Official.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: CORRECTIVE ACTIONS / SANCTIONS

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Corrective Action / Sanctions policy to communicate the Company's willingness and commitment towards enforcing its privacy and security policies and to demonstrate that the Company will hold all teammates accountable for maintaining the privacy of its patients and the security and confidentiality of patient information. Additionally, provides guidelines for addressing intentional and unintentional violations of the Company's Privacy Policies.

POLICY:

The Company will apply the appropriate sanctions against members of its workforce and business associates who fail to comply with the Company's privacy and security policies. These sanctions include the disciplinary actions defined by the People & Culture Department and may result in termination. The People & Culture Department is responsible for documenting the outcomes of all sanctions imposed. Remediation steps outlined in the Business Associate agreement may include termination of the business relationship.

Whether the prohibited conduct constituted simple negligence, gross negligence, or willfulness will be considered in determining and administering the punishment. Intentional or reckless non-compliance will subject transgressors to more serious sanctions. If a teammate or agent has committed a violation of these policies and procedures that might otherwise warrant termination, he or she may nevertheless be subject to a lesser punishment. The decision by the Company to terminate a teammate or agent will be influenced by such mitigating factors as:

A) Whether he or she promptly reported his/her own violation;

B) Whether the report constitutes the Company's first awareness of the violation and the employee's or the agent's involvement; and

C) Whether the employee or agent cooperates fully in investigating and/or correcting the violation.

The Company's decision to impose a punishment less stringent than termination will be left to the sole discretion of the Company.

Discipline resulting from a violation of the Privacy Policies and Procedures will be coordinated through the Privacy Official, and/or the Director of People & Culture. As appropriate, department directors may be required to assist in the disciplinary process.

Another element of a corrective action plan implemented in response to a confirmed deviation from Company policies and procedures, federal or state law, or private payor standards is remedial education. The Privacy Official and the applicable Director of the area will coordinate and develop an effective educational program focused on the problem areas identified. Such education may take the form of individual counseling, a requirement for repeating the online training module or organized training sessions and will be promptly implemented with appropriate teammates or agents to prevent similar problems in the future.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

Envision HEALTHCARE	Ethics & Compliance Department		
	Policy No.: 48	**Created:**	01/2018
		Reviewed:	05/2023
		Revised:	

HIPAA: MITIGATION

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Mitigation policy to communicate the Company's commitment to establishing procedures to correct and prevent violations of a patient's privacy or a breach of the Company's security infrastructure.

POLICY:

The Company will mitigate, to the extent practicable, any harmful effect of a use or disclosure of PHI in violation of its policies and procedures or the requirements of this Security and Privacy Program. The Company is responsible for mitigating harm caused by either members of their workforce or by their business associates.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: WHISTLEBLOWER PROTECTIONS

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Whistleblower Protections policy in order to encourage compliance and enforcement by all Company teammates and mandates that the Company will refrain from retaliatory acts against individuals who file complaints or report a violation as a Whistleblower or as a crime victim.

POLICY:

The Company does not condone and will not allow any retaliatory acts toward any individual including but not limited to patients and teammates for reporting any violation of the Company's privacy policies or a breach of the Company's security infrastructure.

The Company will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual(s) for:

A) Exercising any right under, or for participating in any process established by, HIPAA's privacy rules (Title II, Part 164 Subpart E), including the filing of a complaint with the Company or the Secretary of U.S. Department of Health and Human Services;

B) Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI of the Social Security Act; or

C) Opposing any act or practice made unlawful by HIPAA's privacy rules (Title II, Part 164 Subpart E), provided the individual has a good faith belief that the practice opposed is unlawful and the manner of the opposition is reasonable and does not involve an improper disclosure of PHI.

D) Filing a complaint or reporting a violation related to the Company's privacy and security policies and procedures.

The Company has provided a method for workers to report violations and breaches anonymously. Company employees may use the compliance "Helpline" for reporting incidents (toll-free 877-835-5267).

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: WAIVER OF RIGHTS

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to “teammate” or “teammates” include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates (“Envision” or “the Company”) has adopted this Waiver of Rights policy to communicate that the Company will not condition treatment on a waiver of a patient’s rights to file a complaint with the Secretary of U.S. Department of Health and Human Services for a privacy violation.

POLICY:

The Company will not require its patients to waive their right to file a complaint with the Secretary of U.S. Department of Health and Human Services for any privacy violation as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company’s Ethics & Compliance Program.

	Ethics & Compliance Department		
Envision HEALTHCARE	Policy No.: 51	Created:	01/2018
		Reviewed:	05/2023
		Revised:	

HIPAA: SAFEGUARDS

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Safeguards policy to communicate that the Company will implement organizational safeguards to protect PHI from any intentional or unintentional use or disclosure that violates a patient's right to privacy, and from any threat to the integrity and availability of that information.

POLICY:

A) The Company has developed these administrative procedures, collectively known as "HIPAA Privacy Policies and Procedures." These procedures have been developed to assist employees with regard to guarding the integrity, confidentiality, and availability of PHI. All teammates must be trained on their meaning and application. These procedures must also be periodically evaluated for efficacy and revised when appropriate.

B) The Company will ensure that physical safeguards are in place to guard the integrity, confidentiality and availability of PHI. These safeguards relate to the protection of physical computer systems and devices from intrusion, from environmental hazards, and natural disasters. The Security Official retains authority for compliance with this standard.

C) The Company will ensure that technical security services and mechanisms are in place to guard the integrity, confidentiality, and availability of PHI. Services include processes and tools to control and monitor information access. Security mechanisms will prevent unauthorized access to data that is resident on information systems, and that is transmitted over a communications network. The Security Official retains authority for compliance with this standard.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: DOCUMENTATION OF POLICIES

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Documentation of Policies to ensure that appropriate documentation is created and maintained to document the events associated with the enforcement of the Company's privacy policy.

POLICY:

A) Policies and procedures will be maintained in written or electronic form.

B) If any of these policies require written communication, the Company will maintain such written or electronic communication as documentation.

C) If an action or activity is required by these policies to be documented, the Company will maintain a written or electronic record of such action or activity.

D) All documentation will be retained for six (6) years from the date of its creation or from the date when it was last in effect, whichever is later.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: DEFINITION OF APPROPRIATE ACCESS

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Definition of Appropriate Access policy to define appropriate access levels to the medical record and all related PHI.

POLICY:

A) Access to information in the possession of or under the control of the Company must be provided based on the "need to know" in order to perform their job duties. Accordingly, the Company has established access controls that will restrict access to health information to those employees who have a business need to access it.

B) Business associates will be given access to PHI and/or PHI will be disclosed to them only when there is a legitimate business need for the information and a Business Associate Agreement has been executed.

C) Staff members and business associates must not attempt to access PHI unless they have been granted appropriate access rights and have a clear business reason to do so.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: ASSIGNMENT OF ACCESS PRIVILEGES

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Assignment of Access Privileges policy which requires that access privileges be determined by the departments and assigned based on the need to access information directly related to a worker's duties and responsibilities.

While the Medical Records Department at each facility of the Company or Company's various facility contracts is the true custodian of the medical record, all office-based records are "owned" by the Company. Further, all related billing information, record copies, and other such data delivered or submitted to the corporate offices or other locations for billing purposes is "owned" by the Company. It is the responsibility of the department who generates or warehouses specific information to determine the access rights and security of the information.

POLICY:

Each owner of a specific portion of information must determine which staff members by position and/or responsibility should be given access to such information. Further, the owner is to determine the level of access, including the right to view, amend or include information, or deny access to PHI in its entirety. Questions concerning appropriate access can be directed to the Enterprise Privacy Official.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: REMOTE ACCESS

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Remote Access policy to ensure that all remote access connections associated with the Company's computer systems are established within the guidelines of the Company's information technology security policies and that employees requiring remote access comply with established privacy and security policies.

POLICY:

A) All teammates who perform work remotely will comply with the requirements of the security policy for remote access.

B) No remote connections will be established without the authorization of the Information Technology Department.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

Envision HEALTHCARE	Ethics & Compliance Department		
	Policy No.: 56	**Created:**	01/2018
		Reviewed:	05/2023
		Revised:	

HIPAA: TEAMMATE ACCESS

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Teammate Access policy to inform teammates that, while some teammates may have access to their own computerized medical records, all should be aware they must follow established patient procedures for access.

POLICY:

Company teammates who are also patients are required to comply with the same policies and follow the same procedures as all other patients related to accessing and amending their medical record. They may *no*t use the privileges associated with their position to view their own medical records or related PHI, including billing records, or the records of family or friends.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: PHYSICAL ACCESS TO MEDICAL RECORDS

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Physical Access to Medical Records policy to provide guidelines for securing the physical environment to control access to the paper chart and to information displayed from the electronic chart on a computer monitor.

POLICY:

A) The records of all patients will be compiled in paper-based and/or computerized patient charts. In order to make patient information freely available to staff yet simultaneously prevent access of unauthorized users, patient charts will be stored in, and not be allowed to circulate outside of, restricted areas.

B) Each Department Director is responsible for defining and maintaining appropriate access to the restricted areas within their department.

C) Paper charts should not be left open when not in use, and should not be left unattended in public areas.

D) Computer screens should not positioned for public viewing; when no alternative is available, privacy screens designed specifically for the monitors should be ordered.

E) Electronic records should be closed when not in use.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: RETENTION, DISPOSAL, AND STORAGE

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Retention, Disposal, and Storage policy to provide guidelines to assist with securing and ensuring the safety and privacy of paper charts.

POLICY:

A) The Company has established a formal retention and disposal schedule for medical records information.

B) Disposal of paper, microfiche records, or computerized medical records must be conducted with approved methods.

C) The Company has established a schedule for transporting medical records to long term storage as is appropriate.

D) Short term and long term storage facilities must meet appropriate environmental standards to minimize the risk of damage to the records from water, fire, theft, natural disasters, serious man-made accidents, and other potential threats.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: TEAMMATE PRIVACY RIGHTS

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Teammate Privacy Rights policy to provide guidelines for employees who are also patients of the Company.

POLICY:

Teammates who are patients of the Company must follow standard procedures to obtain or view their own medical records. They also have the same right to privacy and confidentiality as all other patients at the Company.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: NEW TEAMMATE ORIENTATION

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this New Teammate Orientation policy to ensure that all new employees are made aware of the Company security and confidentiality policies.

POLICY:

A) All new teammates, including volunteers, students, physicians, and contract employees, will attend (or participate in a new teammate orientation program in order to receive detailed training about the policies, procedures, and methods of safeguarding the security and confidentiality of patient records. This training will occur as part of their initial orientation & Corporate Compliance Training program.

B) If the New Teammate Orientation schedule does not allow a teammate to attend the orientation prior the worker's start date, the department manager will provide all new teammates with an overview of the teammate's responsibilities related to patient privacy and data security. They will discuss department-specific privacy and security issues and will provide the new teammates with directions on how to access a copy of the Company's privacy policies.

C) New clinicians will also receive detailed training on the policies, procedures, and methods of safeguarding the security and confidentiality of patient records.

D) All teammates are required to take the HIPAA course, at a minimum through the on-line training program.

E) Department directors and/or managers will provide all new teammates whose job responsibility will give them access to PHI, a copy of the department's privacy policies, and discuss any department-specific issues related to privacy and security with the teammate.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: CONTINUING EDUCATION / IN-SERVICE

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Continuing Education / In-Service policy to ensure that on-going educational processes are in place to address changes made to the security and confidentiality policies and procedures.

POLICY:

A) Teammates will receive updates, changes to the policies, procedures, and methods of safeguarding the security and confidentiality of paper-based and computerized patient records as changes occur. Communication methods for these changes or new policies will be based on the magnitude of the changes.

B) Department managers will regularly discuss changes to the policies, procedures, tips, and methods of safeguarding the security and confidentiality of paper-based and computerized patient records as changes occur.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: DISCIPLINE

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Discipline policy to address the specific corrective actions associated with the Company's approach to enforcing its privacy and security policies.

POLICY:

Violations of specific policies and procedures designed to protect the privacy of protected health information shall result in corrective disciplinary action, up to and including termination of employment for cause. Disciplinary actions that may be imposed on Officials, teammates, and agents include verbal or written warnings or reprimand, financial penalties, reassignment to another job, demotion, probation, mandatory education, suspension, and termination from employment. Independent contractors or agents of the Company may be subject to termination of their contract or relationship with the Company among other sanctions.

The discipline taken against a person who violates the provisions of the Company's Privacy Policies and Procedures or federal and state laws, or who have otherwise engaged in wrongdoing, will be determined on a case-by-case basis. Disciplinary action will be taken on a fair and equitable basis. The consequences of non-compliance will be consistently applied and enforced.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: TERMINATION PROCESS

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Terminated employees with access to the Company information technology can do considerable damage. Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Termination Process policy to mitigate this damage by providing guidelines for handling terminations of teammates in an expeditious and prudent manner.

POLICY:

A) In all cases when Company teammates are involuntarily terminated, they must be immediately relieved of all of their duties, required to return all Company equipment and information, and escorted while they pack their belongings and walk out of Company facilities.

B) Managers must terminate workers who have demonstrated that they are a threat to the security of the organization and/or the safety of its teammates.

C) Except when special permission from Executive staff is obtained, all teammates who have stolen Company property, acted with undue insubordination, or been convicted of a felony, must be terminated immediately. Such instant terminations must involve both escort of the individual off Company premises, as well as assistance in collecting and removing the individual's personal effects.

D) In the event that a teammate, volunteer, or consultant is terminating his or her relationship with the Company, the person's immediate manager is responsible for: (1) ensuring all equipment, information, and property in the custody of the person is returned before the person leaves the Company, (2) notifying all administrators handling the computer and communications accounts used by the person as soon as the termination is known, and (3) terminating all other work-related privileges of the person at the time that the termination takes place.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: TEAMMATE DOCUMENTATION

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Teammate Documentation policy to ensure that appropriate documentation is created and maintained to document the events associated with a teammate's corrective action or termination as a result of a violation of the Company's privacy policy.

POLICY:

A) Confidentiality Agreements will be kept with the teammate's P&C file, or the appropriate credentialing file for contractors and physicians.

B) Policies and procedures will be maintained in written or electronic form.

C) If any of these policies require written communication, the Company will maintain such written or electronic communication as documentation.

D) If an action or activity is required by these policies to be documented, the Company will maintain a written or electronic record of such action or activity.

E) All documentation will be retained for seven (7) years from the date of its creation or from the date when it was last in effect, whichever is later.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: PATIENT PRIVACY COMPLAINTS

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Patient Privacy Compliants policy to identify the Company teammates' responsibility with regard to patient complaints about a violation of privacy.

POLICY:

Any patient complaints regarding violations of the patient's right to privacy will be taken seriously and acted upon immediately. Complaints will be reported to their supervisor or directly to the Privacy Official. If reported to the supervisor, he/she will report the violation to the Privacy Official who will initiate the documentation and investigation process.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: REPRODUCTION (COPYING) OF MEDICAL RECORDS

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Reproduction (Copying) of Medical Records policy to define appropriate authorizations for making copies of medical records or other protected health information. The policy further defines guidelines for making copies to protect PHI from unauthorized use or disclosure.

POLICY:

A) The teammate may make copies of a patient's protected health information if they are authorized by the Company.

B) The following types of medical information are typically protected by federal and/or state statute and may NOT be photocopied or faxed without specific patient authorization or where required by law:

(1) Psychotherapy (from records of treatment by a psychiatrist, licensed psychologist, or psychiatric clinical nurse specialist)

(2) Other professional services of a licensed psychologist

(3) Social Work Counseling/Therapy

(4) Domestic Violence Victims' Counseling

(5) Sexual Assault Counseling

(6) Records Pertaining to Sexuality-Transmitted Diseases

(7) HIV Test Results (Patient authorization required for EACH release request.)

(8) Alcohol and Drug Abuse Records Protected by Federal Confidentiality Rules (42 CFR Part 2)

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: E-MAIL OF PROTECTED HEALTH INFORMATION

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this E-Mail of Protected Health Information policy to restrict the e-mail transmission of PHI.

POLICY:

Teammates will refrain from including patient information in electronic mail messages when possible. If the Company identifies an operational process that requires the transmission of PHI, the department manager will take precautions to restrict distribution to those with a need to know and, if email is sent outside the Company, it will be encrypted.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: HANDLING CONFIDENTIAL INFORMATION IN MEETINGS

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Handling Confidential Information in Meetings policy to establish basic guidelines for using PHI during meetings or similar settings in such a way that disclosure of information is not provided unnecessarily to unauthorized individuals.

POLICY:

A) Meetings where PHI is discussed should be attended by individuals who have been specifically invited or by individuals with a specific business purpose for attending. These meetings should be conducted in a secure area such that PHI is not overheard or viewed by unauthorized individuals.

B) All meetings with third party visitors (vendors, customers, regulators, etc.) who are not authorized to have access to PHI must take place in a fully enclosed conference room or office if PHI is being handled by teammates in the immediate vicinity of the meeting room.

C) When PHI has been recorded on black boards or white boards, it must be definitively erased before the authorized recipients of this information leave the area.

D) If documents containing PHI are distributed during the course of the meeting, and those documents are not required by the recipient for health care operations, the documents must be collected and destroyed at the completion of the meeting.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: CONFIDENTIAL INFORMATION AND EQUIPMENT IN PUBLIC AREAS

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Confidential Information and Equipment in Public Areas policy to encourage departments to be vigilant in ensuring that PHI is not inappropriately used or disclosed through the inappropriate use or location of equipment or other confidential materials.

POLICY:

A) Departments must not position any equipment, including telephones, workstations, fax machines, copiers, and printers in public areas such that PHI may be overheard or viewed by unauthorized individuals.

B) The display screens for all PCs, workstations, and dumb terminals used to handle sensitive data must be positioned such that they cannot be readily viewed through a window, by persons walking in a hallway, or by persons waiting in reception and related public areas.

C) Fax machines and computer printers used to print sensitive data must be located in such a manner that the printouts cannot be readily viewed through a window, by persons walking in a hallway, or by persons waiting in reception and related public areas.

D) Teammates who work on transportable computers (portables, notebooks, laptops, palmtops, etc.) and paper records should also be cognizant of their position with regard to unauthorized viewing of PHI.

E) Teammates should make every effort to conceal or screen paper charts, medical records, faxes, and other documentation containing PHI. Electronic records should be closed or screened when not needed for access. Verbal communication should be conducted in the most discreet manner possible.

F) Computer printouts, faxes, medical records, and other paper records should not be left in open work areas so as to expose the contents of the records. Files and papers should be put away when not in use.

G) Medical Records and charts should be kept and updated in appropriately designated areas.

H) File cabinets should be locked when not appropriately supervised.

I) Faxes, computer printouts, and copies/originals should be collected as soon as possible and appropriately filed.

J) All activities pertaining to sensitive information must take place in areas that are physically secured and protected against unauthorized access, interference, and damage.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: REPORTING STRUCTURE – PRIVACY OFFICIAL

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Reporting Structure – Privacy Official policy to identify a single point of contact in dealing with complaints and violations of policy related to privacy issues.

POLICY:

A) The Company Privacy Official is responsible for the development, implementation, and enforcement of the confidentiality policies and procedures. Any questions, concerns, reports, or complaints should be directed to the Privacy Official.

B) Company teammates will direct any complaints, including patient complaints, and reports of a violation related to the Company's privacy and security policies to the Privacy Official. The Privacy Official will coordinate and initiate an investigation of the complaint or violation.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: COMPLIANCE HELPLINE

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Compliance Helpline policy to provide another alternative for reporting privacy violations and security breaches, and to ensure anonymity for the reporting individual.

POLICY:

Teammates may use the Company's Ethics and Integrity Helpline to file a complaint or report related to a violation of the Company's privacy policies or a breach of the Company's security infrastructure.

The Compliance Department's Ethics and Integrity Helpline # is 877-835-5267.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: DOCUMENTATION OF PRIVACY MATTERS

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Documentation of Privacy Matters policy to require that any discovery of a violation of privacy policies or a breach of security must be documented.

POLICY:

Company Directors must ensure that documentation exists for any incident and related action taken relative to the Company's privacy policies. Specifically, Directors will:

A) Collect all written patient requests related to accessing and amending their medical records, accounting of disclosures, restrictions on use or disclosures, confidential communications, and notification to other involved in the patient's care;

B) Document incidents of privacy policy violations and breaches of the Company's security infrastructure; and

C) Provide copies of this documentation to the Privacy Official, as received.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: REPORTING AND INVESTIGATING SUSPECTED BREACHES

SCOPE:

All Envision Healthcare teammates. For purposes of this policy, all references to "teammate" or "teammates" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Reporting and Investigating Suspected Breaches policy to ensure that standards are developed and employed for reporting and responding to an incident involving the breach of Unsecured Protected Health Information or a breach of Personal Information, as those terms are defined in this policy and in the HIPAA Privacy and Security rules.

POLICY:

Breaches of Unsecured Protected Health Information

The Company will comply with all applicable laws and regulations to determine when the Company must notify patients that a breach of that patient's Unsecured PHI has occurred.

A) A breach of Unsecured PHI is the unauthorized acquisition, access, use, or disclosure of Unsecured PHI in a manner which compromises the security or privacy of the PHI. An unauthorized access, use, or disclosure of Unsecured PHI is presumed to be a breach unless the Company can demonstrate that there is a low probability that the PHI has been compromised. The Company's Privacy Official, in conjunction with others designated by the Privacy Official, is responsible for making the determination on the probability of compromise.

   (1) Unsecured PHI means all information that is not encrypted according to the Company's standards, has not been shredded or has not, in some other way, been made unusable or unreadable to unauthorized individuals.

   (2) A breach does not include (i) unintentional acquisition, access, or use of PHI by a member of the Company's workforce or a Company Business Associate if the acquisition, access, or use was made in good faith and would otherwise be within the scope of the workforce member's (or the Business Associate's) scope of authority as long as there is no further inappropriate use or disclosure; or (ii)

an inadvertent disclosure by a person who is authorized to access PHI at the Company to another person who is authorized to access the Company PHI provided there is no further inappropriate uses or disclosures.

(3) A disclosure of PHI where the Company has a good faith belief that the unauthorized person who received the information would not reasonably be able to retain the information.

B) A breach of Unsecured PHI can also be a "security incident." Security incidents include unauthorized probing and browsing, disruption or denial of service, altered or destroyed input, processing, storage, or output of information, or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent. Security incidents include, but are not limited to, detection of virus, worm, adware, spyware, trojan horse and/or any malware, unauthorized use of computer accounts and computer systems, as well as complaints of improper use of information resources. Additional examples of possible incident categories include: compromise of system integrity, denial of system resources, illegal access to a system (either a penetration or an intrusion), malicious use of system resources, or any kind of damage to a system.

C) If any member of the Company's workforce discovers or suspects that there has been a breach of Unprotected PHI, he/she should report the matter to the Privacy or Security Official immediately.

D) If a teammate is uncertain whether a particular situation would be a breach, he/she should contact the Privacy Official immediately. Examples of activity that might need further investigation include:

(1) If a teammate notices records containing PHI in a location other than where they are to be properly stored, such as in trash receptacles, recycle bins, or other locations, the teammate should notify his/her supervisor or the Privacy Official.

(2) If a teammate notices:

(a) His/her computer is running a strange process;

(b) Someone trying to log into his/her computer;

(c) That his/her computer has a virus;

(d) Lost or missing equipment;

(e) New unauthorized equipment suddenly appears.

E) The Privacy Official will investigate the report and make a determination as to whether the situation reported constitutes a breach of Unsecured PHI. When investigating the incident, the Privacy Official will determine whether the Company has reporting obligations to an individual or to a client. In determining whether the incident is or is not a breach of Unsecured PHI, the Privacy Official will determine whether there is a low probability that the PHI has been compromised. In making his/her determination, the Privacy Official will take into consideration:

(1) The type of information inappropriately used or disclosed;

(2) The characteristics of the recipient of the information;

(3) Whether the PHI was actually acquired or viewed;

(4) The ability to mitigate the inappropriate disclosure.

F) The Privacy Official will log all pertinent information regarding the situation.

Notice

If the Privacy Official determines a breach of Unsecured PHI has occurred, the Privacy Official will notify affected individuals as soon as possible, and no later than sixty (60) days after the initial discovery of the breach.

A) The Notice to Individuals will include:

(1) A brief description of the breach including the date of the breach and the date of the discovery of the breach, if known;

(2) A description of the information that was compromised (for example whether the information included a full name, account number, diagnosis, or some other type of information);

(3) Information on steps the individual can take to protect him or herself from potential harm resulting in from the breach;

(4) A brief description of actions taken by the Company to investigate the breach, to mitigate harm, and to protect against any further breaches; and

(5) Contact procedures for individuals to ask questions or learn of additional information (which must include a toll-free telephone number, an email address, a website, or a postal address).

B) Notice will be sent by the Company's Privacy Official and will be sent in writing by first-class mail to the individual, or if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail.

C) If the Company has insufficient or out-of-date contact information, the Company will attempt to identify a substitute form of notice to reach the individual. If there is insufficient or out of date contact information for fewer than ten (10) individuals, then substitute notice may be provided by telephone, an alternative form of written notice, or other means.

D) If there is insufficient or out of date contact information for more than ten (10) individuals, the substitute notice must be either:

(1) In the form of a conspicuous posting for a period of ninety (90) days on the home page of the Company's web site; or

(2) A conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside.

In both cases, the notification must include a toll-free phone number that remains active for at least ninety (90) days where an individual can learn whether the individual's Unsecured PHI may be included in the breach.

E) If the substitute notice must occur by telephone, the Privacy Official or designated person giving notice should limit disclosure of PHI until the Privacy Official or designated person can confirm with reasonable certainty that the person on the phone is the individual affected.

F) If the case is deemed to require urgency because of the potential for misuse of the information, the Privacy Official may provide information by telephone or other means in addition to the written notice above.

G) If a breach of Unsecured PHI involves more than five hundred (500) residents of a state or jurisdiction, the Privacy Official will notify prominent media outlets serving the state or jurisdiction. The media notification must be given without unreasonable delay and in all cases must be given within sixty (60) days after discovery of the breach involving more than five hundred (500) residents of a state.

H) If the breach involves Unsecured PHI of five hundred (500) or more individuals, the Privacy Official will provide notice to the Secretary of U.S. Department of Health and Human Services ("HHS") at the same time as notice is provided to the affected individuals and in the manner specified on the HHS website.

I) If the breach involves Unsecured PHI of fewer than five hundred (500) individuals, the Privacy Official will maintain a log or other documentation of such breaches and, not later than sixty (60) days after the end of each calendar year, provide the required notification to the Secretary of the U. S. Department of Health and Human Services for breaches occurring during the preceding calendar year, in the manner specified on the HHS website.

J) If a law enforcement official states to the Company or a Business Associate of the Company that a notification, notice, or posting otherwise required by law would impede a criminal investigation or cause damage to national security, the Company will comply with the following standards:

(1) If the statement is in writing and specifies the time for which a delay is required, the Privacy Official will delay such notification, notice, or posting for the time period specified by the law enforcement official; or

(2) If the statement is made orally, the Privacy Official will document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than thirty (30) days from the date of the oral statement, unless the law enforcement official provides a written statement as described above.

Breaches of Personal Information

The Company will comply with all applicable laws and regulations to determine when the Company must notify patients that a breach of that patient's PHI has occurred.

A) The Company will reevaluate any applicable state law requirements if there is a breach that includes computerized personal information or PHI. State law requirements will vary and often depend on the state of residence of the patient. Therefore, employees should report all suspected breaches to the Privacy Official.

B) While state law requirements vary, generally states define personal information to include a person's name in conjunction with a social security number or other identification number (such as a driver's license number) or a person's name in conjunction with an account number or credit card number in combination with a required security code or access code.

C) The Company's Privacy Official will evaluate whether the potential breach includes a breach of personal information that may require notification under applicable state laws.

IT Staff Surveillance

IT staff will remain alert to signs that may signal security incidents or breaches of electronic PHI have occurred or are occurring. Those signs include, but are not limited to, the following:

A) The network intrusion detection sensor alerts when a buffer overflow attempt occurs against an FTP server;

B) The antivirus software alerts when it detects that a host is infected with a worm;

C) The Web server crashes;

D) Users complain of slow access to hosts on the Internet;

E) The system administrator sees a filename with unusual characters;

F) The user calls the appropriate Beta 5 personnel to report a threatening e-mail message;

G) The host records an auditing configuration change in its log;

H) The application logs multiple failed login attempts from an unfamiliar remote system;

I) The e-mail administrator sees a large number of bounced e-mails with suspicious content; and

J) The network administrator notices an unusual deviation from typical network traffic flows.

The IT staff will also be vigilant to common precursors to an attack, including the following:

A) Unusual port scans of a group of targeted hosts;

B) Web server log entries that show the usage of a Web vulnerability scanner;

C) An announcement of a new exploit that targets a vulnerability of the Company's mail server; and

D) A threat from a hacktivist group stating that the group will attack the organization.

Closing an Investigation

The Privacy Official will create a report once the investigation is complete.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.

HIPAA: INFORMATION BLOCKING

SCOPE:

Applies to all Envision Healthcare colleagues. For purposes of this policy, all references to "colleague" or "colleagues" include temporary, part-time and full-time employees, independent contractors, clinicians, officers and directors.

PURPOSE:

Envision Healthcare and its subsidiaries and affiliates ("Envision" or "the Company") has adopted this Information Blocking policy to (i) address the effect of the Information Blocking Rules on disclosures of EHI (as defined below) permitted by HIPAA and these HIPAA policies; (ii) describe a process for determining whether such disclosures are required by the Information Blocking Rules; and (iii) describe a process for determining whether any exceptions to the Information Blocking Rules permit the Company to deny a request for EHI otherwise permitted by HIPAA.

DEFINITIONS:

A. *EHI* or *Electronic Health Information* means electronic PHI included in a designated record set (as defined by HIPAA), regardless of whether the group of records are used or maintained for a Covered Entity. EHI does not include: (i) psychotherapy notes (as defined in 45 CFR 164.501); or (ii) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. Until May 2, 2022, EHI is limited to the EHI identified by the data elements represented in the United States Core Data for Interoperability ("USCDI") standard adopted in 45 CFR § 170.213.

B. *Information Blocking Rules* means the rules prohibiting practices likely to interfere with, prevent, or materially discourage access, exchange or use of EHI held on behalf of a covered entity or any other entity as set forth at 45 CFR § 171.100, *et seq*.

C. *Practice* means an act or omission by the Company. For purposes of this policy, examples of Practices include denying requests to access, use, or exchange EHI; charging fees for access, use, or exchange of EHI; or the manner in which access, use, or exchange of EHI is provided.

POLICY:

A. *In General*

The Company's Practices, including uses and disclosures of EHI, must be in accordance with the HIPAA Policies, HIPAA, and the Information Blocking Rules. Whereas HIPAA *permits* the Company to access, use, and exchange EHI for certain purposes, the Information Blocking Rules *require* the Company to do so unless an exception applies.

Section IV(C) of this policy lists the Company's HIPAA Policies that address and describe the conditions for uses and disclosures of PHI that are permitted under HIPAA.

Section IV(D) of this policy sets forth the Company's process for reviewing Practices, including denials of requests for access to, or the use or exchange of, EHI.

Before implementing a Practice, including declining to make a requested use or disclosure of EHI, that is permitted under a policy listed in Section IV(C), the review process in Section IV(D) must be done to ensure that any Practice does not violate the Information Blocking Rules.

B. *Standards for Information Blocking*

When Company receives a request for EHI (for example: a patient requests access to or a copy of their EHI; an unaffiliated treating provider requests information relating to a patient's health outcomes; a health plan requests information relating to a member's claims) or otherwise engages in a Practice (for example: having a policy in place that patient consent is required to share EHI with other treating providers, even if permitted by law without consent; requiring community physicians to adopt the same EMR as Company or otherwise revoking admitting privileges), if the Practice is able to meet an exception as described in Section II(D)(3) below, it will not be considered information blocking as the exceptions act as "safe harbors" under the Information Blocking Rules.

Where a Practice does *not* meet a safe harbor as described below, it is not automatically a violation of the Information Blocking Rules. To be considered information blocking, the Company must:

1. Know that a Practice is
2. Unreasonable and
3. Likely to interfere with, prevent, or materially discourage the access, exchange or use of EHI.

In addition, the Information Blocking Rules also contain other exceptions not discussed in this Policy because they are unlikely to apply to Company's operations (such as Practices by Health IT Developers that involve system downtime or otherwise making EHI unavailable through their Health IT systems). Workforce members who have questions about whether any exceptions to the Information Blocking Rules apply must contact the Privacy Official before denying requests for access, use, or exchange of EHI or otherwise implementing a Practice.

The Privacy Official will document details regarding any decision-making process when denying requests to access, use, or exchange EHI (or otherwise engaging in a Practice) when an exception does not apply. See Section F for more information regarding documentation.

C. *Situations in which the Use or Disclosure of PHI is Permitted under HIPAA*

HIPAA *permits* the use and disclosure of PHI, including EHI, as set forth and under the conditions described in the policies listed below.

Policy No.	Policy Title
4	Minimum Necessary / Need to Know
6	Disclosing Protected Health Information for Health Care Operations
7	Disclosing Protected Health Information for Treatment
8	Disclosing Protected Health Information as Required By Law
9	Disclosing Protected Health Information About Decedents
10	Disclosing Protected Health Information for Judicial and Administrative Release
11	Disclosing Protected Health Information to Law Enforcement
12	Disclosing Protected Health Information About Victims of Abuse, Neglect, or Domestic Violence
14	Disclosing Protected Health Information For Minors to a Parent or Legal Guardian
15	Disclosing Protected Health Information to Family / Friends / Caregivers
16	Disclosing Protected Health Information for Workers Compensation / Employers
17	Disclosing Protected Health Information for Public Release
18	Disclosing Protected Health Information for Specialized Government Functions
19	Uses and Disclosures of Protected Health Information for Research
20	Using and Disclosing Protected Health Information for Marketing
21	Fundraising
22	Prohibition on Sale of Protected Health Information
23	Business Associates

25	Restriction of Use or Disclosure
Policy No.	Policy Title
26	Alternative / Confidential Communications
27	Request and Documentation for Access
29	Provision of Access
32	Provision of Amendment
38	Verification of Person(s) Requesting Protected Health Information
39	Authorization Requirements

D. *Process for Reviewing Practices, including Potential Denials of Requests for EHI*

When a Practice, including a use or disclosure of EHI pursuant to a request, is not prohibited by one of the policies set forth above, but the Company is considering denying the request (or implementing other Practices), the Company must follow the process described in this Section IV(D) to ensure that any such Practice, including a denial, meets an exception to or would otherwise not be considered information blocking (see Section IV(B)).

1. <u>*Step One: Is the request for, or does the Practice otherwise involve, EHI*</u>? These requirements do not apply to Practices relating to, or requests for, information that is not EHI as described above. Colleagues should consult with the Privacy Official if they are unclear as to whether the PHI at issue is covered by this policy.

2. <u>*Step Two: Is the requested access, use or disclosure required by law*</u>? If access, use or disclosure is required by HIPAA (*e.g.,* disclosures of PHI to HHS for determining compliance with the HIPAA rules; disclosures of PHI to individuals pursuant to an access request) or required by other applicable law (*e.g.,* state law requires reporting gunshot wounds to law enforcement or reporting suspected abuse to a public health authority), Company will comply with the request. Colleagues should ensure that any such disclosure or use meets the requirements of such law and *HIPAA Policy #8 – HIPAA: Disclosing Protected Health Information as Required by Law* and *HIPAA Policy # 11 – HIPAA Disclosing Protected Health Information to Law Enforcement*. Colleagues should also review Step Three (below) to ensure that Practices involved in making the disclosure (such as fees imposed for access, or the content and manner of access) do not constitute information blocking or meet an exception.

3. *Step Three: Can a Practice, including a denial of a request for EHI, meet an Information Blocking exception?* If the request relates to EHI, and the requested access, exchange, use, or disclosure is permitted by HIPAA but not required by HIPAA or other law, the Company may deny the request or otherwise engage in a Practice with respect to such EHI if one of the exceptions set forth below is met.

a. Privacy Exception. The Information Blocking Rules do not require the Company to provide access, exchange, or use of EHI in a manner that would violate HIPAA or other laws. The Privacy Exception

permits the Company to engage in a Practice (including denying a request for EHI) in order to protect an individual's privacy provided certain requirements are met (*i.e.*, simply concluding that another Company HIPAA policy does not permit a disclosure is not alone sufficient). To meet this exception, one of the following sub-exceptions must be met:

1) Sub-Exception One: Precondition not satisfied. This sub-exception covers Practices, including denial of a request to access, exchange, use or disclose EHI, on the basis that preconditions required by HIPAA or other applicable law have not been met; put another way, denying the request is required by law because a requirement has not been met. Examples include: a scenario where HIPAA requires an authorization for a disclosure of EHI for research (because no research exception is met), but the patient refuses to sign an authorization; state law requires written patient consent for a disclosure of substance abuse treatment records to an insurer, but no consent has been obtained; or HIPAA requires Company to verify the identity and authority of a requestor, and verification documentation is not provided. The following requirements apply to meet Sub-Exception One:

a) If the applicable precondition to a disclosure, access or use of EHI is a consent or authorization form from an individual, but the Company has received such form that does not satisfy all required elements of the applicable law, the Company must use reasonable efforts within its control to provide the individual with a form that satisfies all required elements of the precondition. This does not mean Company must take all possible action to "chase down" a compliant consent or authorization; however, Company must take reasonable steps, such as notifying the requestor of the elements that are missing. In addition, Company must not improperly encourage or induce the individual (patient or personal representative) to withhold the consent or authorization.

b) Regardless of which type of requirement or precondition has not been met, Company's Practice (including denial of a request) must:

i Be tailored to the requirement that has not been satisfied. For example, if Company denies a request on the basis that the requestor's identity cannot be verified, this determination may not be based on unreasonably onerous requirements (such as a requirement that only a valid driver's license may be used to verify one's identity, when other valid forms of ID are available), but rather based on Company's policy for verification;

ii Be implemented in a consistent and nondiscriminatory manner, meaning workforce members follow the steps outlined in this Sub-Exception One in the same manner regardless of who is requesting the EHI; and

iii Either (I) conform to documented HIPAA Policies which specify the criteria for determining when the precondition is satisfied and, as applicable, the steps Company will take to satisfy the precondition and are implemented by Company, including through training on the applicable policies; or (II) be documented by the Company, on a case-by-case basis, identifying the criteria used by Company to determine when the precondition would be satisfied, any criteria that were not met, and the reason why the criteria were not met. Company may use this Sub-Exception One for atypical requests and other unique scenarios that are not addressed in these policies. For example, if Company has EHI for multiple individuals with the same full name, Company may deny an EHI request on the basis of protecting the individuals' privacy if Company documents its process for determining the correct individual could not be appropriately identified, including documentation of the criteria described above.

c) Company may rely, for purposes of meeting the requirements of subsection (b) of this *Sub-Exception One*, on a uniform set of policies that are designed to meet the requirements of one state in which Company operates, provided such policies address the more restrictive preconditions of the states in which Company operates.

2) Sub-Exception Two: Denial consistent with HIPAA right of access. This sub-exception permits the Company to deny a request to access, exchange, use or disclose EHI if the Company would be permitted to deny an individual's request to access or for a copy of the same information, as set forth in *HIPAA Policy #28 – HIPAA: Denial of Request for Access*, sections A and D.

3) Sub-Exception Three: Respecting an individual's request not to share information. The Company may deny a request to access, exchange, use or disclose EHI on the basis that the patient has requested that the EHI not be shared if the provisions below are met:

a) The individual requests that Company not provide the individual's EHI (which may include requests for restriction pursuant to *HIPAA Policy #25 – HIPAA: Restriction of a Use or Disclosure*).

b) The request was made without any improper encouragement or inducement by the Company. For example, the Company may not discourage individuals from sharing information with other, unaffiliated providers on the basis of speculative risks to their EHI, and the Company will not provide any forms to individuals for restriction requests that are not written in plain language understandable to the individual;

c) The Company documents the request within a reasonable period of time (note: once Company has documented such request with a reasonable period of time, it need not repeatedly re-confirm and redocument the request); and

d) The Company implements the process in this Section in a consistent and non-discriminatory manner.

The Company may terminate an individual's request that the EHI not be shared in accordance with the requirements set forth in *HIPAA Policy #25 – HIPAA: Restriction of a Use or Disclosure*.

b. Security Exception. The Company may engage in a Practice (including denying a request to access, use, or exchange EHI) in order to protect the security of such EHI, provided:

1) The Practice is directly related to safeguarding the confidentiality, integrity, and availability of EHI (for example, the Company denies a request because it is aware of a specific ongoing security incident or security threat);

2) The Practice is tailored to the specific security risk being addressed;

3) If the Practice is based on a Company security policy, the policy must: (A) be in writing; (B) have been prepared on the basis of, and is directly responsive to, security risks identified and assessed by or on behalf of the Company (such as the Company's most recent HIPAA security risk analysis); (C) align with one or more applicable consensus-based standards or best practice guidance; and (D) provide

objective timeframes and other parameters for identifying, responding to, and addressing security incidents; and

4) If the Practice does not follow a Company security policy, the Company must have made a determination, based on particularized facts and circumstances, that: (A) the Practice is necessary to mitigate the security risk to EHI; and (B) there are no reasonable alternatives to the Practice that address the security risk that are less likely to interfere with, prevent, or materially discourage access, exchange or use of EHI.

5) The Company must implement the Practice in a consistent and non-discriminatory manner.

c. <u>Infeasibility Exception</u>. The Company may deny a request to access, use, or exchange EHI due to the infeasibility of the request, provided one of the following conditions is met:

1) The Company cannot fulfill the request due to a natural or human-made disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil, or regulatory authority;

2) The Company cannot fulfill the request because the Company is unable to segment the requested EHI from information that cannot be made available due to an individual's preference or because the EHI cannot be made available by law; or

3) The Company demonstrates, prior to responding to the request, through contemporaneous written documentation, its consistent and non-discriminatory consideration of the following factors that led to its determination of infeasibility: (A) the type of EHI and the purposes for which it may be needed; (B) the cost to the Company of complying with the request in the manner requested; (C) the financial and technical resources available to the Company; (D) whether the Company's practice is non-discriminatory and the Company provides the same access, exchange, or use of

EHI to its companies or to its customers, suppliers, partners, and other persons with whom it has a business relationship; (E) whether the Company owns or has control over a predominant technology, platform, health information exchange, or health information network through which electronic health information is accessed or exchanged; and (F) why the Company was unable to provide access, exchange, or use of EHI consistent with the Content and Manner Exception (addressed below). In determining whether the above circumstances are infeasible, the Company will not consider whether the manner requested would have facilitated competition with the Company or prevented the Company from charging a fee or resulted in a reduced fee.

If the Company denies a request for EHI based on the Infeasibility Exception, the Company shall, within ten (10) business days of the request, provide to the requestor in writing an explanation of why the request is infeasible (e.g., uncontrollable events, segmentation restrictions, or circumstances otherwise making the request infeasible).

d. Preventing Harm Exception. The Company may engage in a Practice (including denying a request to access, use, or exchange EHI) provided the Practice is reasonable and necessary to prevent harm to a patient or another person. For purposes of this Preventing Harm Exception, "patient" means the person who is the subject of the EHI. The following requirements must also be met:

1) The Company must hold a reasonable belief that denying the request to access, use or exchange EHI (or otherwise engaging in a Practice that is likely to interfere with access to or exchange or use of EHI) will substantially reduce a risk of harm to a patient or other person that would otherwise arise from such access, use, or exchange.

2) Type of risk. The risk of harm posed to the patient or other person must: (A) be determined on an individualized basis in the exercise of professional judgment by a licensed health care professional who has a current or prior clinician-patient relationship with the patient. This individualized risk determination must be documented in the patient's medical record. Documentation in the EMR may be sufficient but is

not required. Colleagues other than the health care professional making the risk determination (such as the Privacy Official) may rely on such professional's determination of a risk of harm; <u>or</u> (B) arise from data known or reasonably suspected by Company to be misidentified or mismatched, corrupt due to technical failure, or otherwise erroneous.

3) Where the risk of harm is based on an individualized basis in the exercise of professional judgment by a licensed health care professional, as described in Section (IV)(D)(3)(d)(2)(A) above, the Company must implement the Practice (i.e., making the denial) in a manner consistent with any rights the patient has to review a denial of access (*see HIPAA Policy #28 – HIPAA: Denial of Request for Access*, section C) or any federal, state, or tribal law, to have the determination reviewed and potentially reversed.

4) Type of harm. The type of harm the Practice is meant to substantially reduce must be one that could serve as grounds for the Company to deny a patient (or personal representative) <u>access</u> to his or her PHI (*see HIPAA Policy #28 – HIPAA: Denial of Request for Access*). There are three types of harm that

serve as such grounds for denial of access, as illustrated in the circumstances described below:

a) The request for EHI is from a patient's personal representative, and the denial (or other Practice that is reasonably likely to interfere with the personal representative's access, exchange or use of EHI) is based on a licensed health care professional's individualized determination of the risk of harm from providing access to such personal representative. The *type of harm* in this circumstance is substantial harm to the patient or another person (*see HIPAA Policy #28 – HIPAA: Denial of Request for Access,* section (B)(3)).

b) The request for EHI is from a patient or personal representative, and the denial (or other practice that will interfere with the patient's or personal representative's access, exchange, or use of EHI) is based on a licensed health care professional's individualized determination of the risk of harm from providing such access. The *type of harm* in this circumstance is substantial harm to another person (other than a treating provider) to whom reference is made in the requested PHI (*see HIPAA Policy #28 – HIPAA: Denial of Request for Access,* section (B)(2)).

c) The request for EHI is from a patient, and the denial (or other Practice that is reasonably likely to interfere with the patient's access, exchange or use of their own EHI) is based either on a licensed health care professional's individualized determination of the risk of harm from providing such access or arising from data known or reasonably suspected to be corrupt, erroneous or misidentified due to technical failures. The *type of harm* in this circumstance is harm to the life or physical safety of the patient or other person (*see HIPAA Policy #28 – HIPAA: Denial of Request for Access,* section (B)(1)).

d) The request for EHI is from a patient's personal representative, and the denial (or other Practice that is reasonably likely to interfere with the personal representative's access, exchange or use of EHI) is based on reducing the risk of harm arising from data known or reasonably suspected to be corrupt, erroneous or misidentified due to technical failures. The *type of harm* in this circumstance is harm to the life or physical safety of the patient or other person (*see HIPAA Policy #28 – HIPAA: Denial of Request for Access,* section (B)(1)).

5) The Company's denial (or other Practice that is reasonably likely to interfere with the access, exchange, or use of EHI) must be consistent with a Company policy that meets the

requirements set forth below in subsection (a) - or, in the absence of a Company policy applicable to the denial or to its use in particular circumstances, the Practice must be based on a determination that meets subsection (b) below.

a) The Company policy must: be in writing; be based on relevant clinical, technical, and other appropriate expertise; be implemented in a consistent and nondiscriminatory manner; and conform each Practice (*i.e.* each denial of a request for access to or use or exchange of EHI) to the conditions in this Section IV(D)(3)(d) (and with respect to the "type of risk" and "type of harm," only those conditions that are applicable).

b) Alternatively, a determination must: be based on facts and circumstances known or reasonably believed by Company at the time the determination was made; and be based on expertise relevant to implementing the Practice (*i.e.* denying the request for access to or use or exchange of EHI) consistent with the conditions in this Section IV(D)(3)(d) (and with respect to the "type of risk" and "type of harm," only those conditions that are applicable.

6) If Company lacks the technical capability to sequester only the EHI that Company reasonably believes poses a risk of harm from other EHI subject to the request, this Preventing Harm Exception is not applicable. Instead, Company should review the Content and Manner Exception or the Infeasibility Exception set forth in this Policy.

7) The Practice under the <u>Preventing Harm Exception</u> must be no broader than necessary to substantially reduce the risk of harm that the denial is meant to reduce.

e. <u>Content and Manner Exception</u>. The Company may limit the content of its response to a request to access, exchange, or use EHI or the manner in which it fulfills a request to access, exchange, or use EHI, provided the following conditions are met:

1) As described in the "Definitions" section, until May 2, 2022, "EHI" is limited to data elements represented in the United States Core Data for Interoperability (USCDI) standard adopted in § 170.213. Until that date, if there is no available information blocking exception and the requested access to or use or exchange of EHI is permitted by HIPAA and other applicable law, the Company must provide such access, use or exchange using the data elements in the USCDI standard. For requests on or after May 3, 2022, the Company must provide EHI without the USCDI limitation.

2) The Company must fulfill a request in any manner requested unless the Company is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request.

3) If the Company is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request, the Company must fulfill the request in an alternative manner, without unnecessary delay, pursuant to the following steps, in order of priority. The Company will start with option (A) and only proceed to the next option if the Company is technically unable to fulfill the request in the manner identified in the option: (A) using technology certified to standard(s) adopted in 45 CFR Part 170 that is specified by the requestor; (B) using content and transport standards specified by the requestor and published by: (1) the Federal Government; or (2) a standards developing organization accredited by the American National Standards Institute; and (C) using an alternative machine-readable format, including the means to interpret the EHI, agreed upon with the requestor.

4) Any fees charged by the Company in relation to fulfillment of a request are required to satisfy the Fees Exception set forth below, and any license of interoperability elements granted by the Company in relation to fulfillment of the request is required to satisfy the licensing exception to the Information Blocking Rules in 45 CFR § 171.303 (unless the Company is able to reach agreeable terms with the requestor). Colleagues must contact the Privacy Official to

ensure compliance with such additional exceptions, to the extent applicable.

f. Fees Exception. The Company may charge fees, including fees that result in a reasonable profit margin, for accessing, exchanging, or using EHI provided the following conditions are met:

1) The fees the Company charges must be:

a) based on objective and verifiable criteria that are uniformly applied for all similarly situated classes of persons or entities and requests;

b) reasonably related to the Company's costs of providing the type of access, exchange, or use of EHI to, or at the request of, the person or entity to whom the fee is charged;

c) reasonably allocated among all similarly situated persons or entities to whom the technology or service is supplied, or for whom the technology is supported; and

d) based on costs not otherwise recovered for the same instance of services to a provider and third party.

2) The fees that the Company charges must not be based on:

a) whether the requestor or other person is a competitor, potential competitor, or will be using the EHI in a way that facilitates competition with the Company;

b) sales, profit, revenue, or other value that the requestor or other persons derive or may derive from the access, exchange, or use of the EHI;

c) costs that the Company incurred due to health IT being designed or implemented in a non-standard way, unless the requestor agreed to the fee associated with the non-standard design or implementation to access, exchange, or use the EHI;

d) costs associated with intangible assets other than the actual development or acquisition costs of such assets;

e) opportunity costs undervalued to the access, exchange, or use of EHI; or

f) any costs that led to the creation of intellectual property if the Company charged a royalty for that intellectual property pursuant to the licensing exception to the Information Blocking Rules in § 171.303 and that royalty included the development costs for the creation of the intellectual property.

3) Colleagues should consult with the Privacy Official before imposing or seeking to charge any fee for access, use, or exchange of PHI to ensure compliance with the Information Blocking Rules. Such fees or Practices include charging fees:

a) For labor, copying, postage, or other costs in connection with an individual's access or a copy of his or her PHI (*see HIPAA Policy #29 – HIPAA: Provision of Access*);

b) Based in part on the electronic access of an individual's EHI by the individual, their personal representative, or another person or entity designated by the individual;

c) To perform an export of EHI via the capability of health IT certified to 45 CFR § 170.315(b)(10)[2] for the purposes of switching health IT or to provide patients their EHI; and

[2] Rule forthcoming as of August 2020.

d) To export or convert data from an EHR technology that was not agreed to in writing at the time the technology was acquired.

E. Documentation

Information required to be documented by this policy shall be recorded and be maintained for six (6) years from the date of its creation or the date it is last in effect, as applicable. In addition, where this policy specifies additional or new documentation requirements (such as when necessary to meet a particular exception or sub-exception to the Information Blocking Rules), the Privacy Official will ensure that such documentation is maintained for six (6) years from the date of its creation or the date it is last in effect, whichever is longer.

F. Additional Requirements

The decision-making process outlined in this policy must be followed in a manner consistent with the Company's other HIPAA policies regarding the use and disclosure of PHI. For example, the minimum necessary standard applies, as described in *HIPAA Policy #4 – HIPAA: Minimum Necessary / Need to Know*; (ii) the identification rules outlined in *HIPAA Policy #38 – HIPAA: Verification of Person(s) Requesting Protected Health Information* apply, and (iii) the safeguards outlined in *HIPAA Policy #51 – HIPAA: Safeguards* must be observed.

POLICY REVIEW

The Ethics & Compliance Department will review and update this Policy, when necessary, in the normal course of its review of the Company's Ethics & Compliance Program.