
# Rayaf Health

***HIPAA Privacy***

***Policy and Procedure Manual***

RAYAF HEALTH

# Contents

RAYAF HEALTH

# Overview

Rayaf Health is a healthcare organization; Rayaf Health team members have access on a daily basis to a significant amount of information about our patients and their parents and guardians, much of which contains confidential and sensitive health information.

It is our legal and ethical responsibility to protect the confidentiality of this information. Compliance with this Privacy Policy will ensure that patients' and their family's personal health information ("PHI") is protected and used only for appropriate purposes. A commitment to maintaining the privacy of personal health information will assure the confidence of the families we serve and the continued success of our organization.

This Privacy Policy was developed to assure compliance with the Privacy Rule of the Health Insurance Portability and Accountability Act ("HIPAA") and other state and federal regulations regarding privacy.

# Definitions

## Protected Health Information (PHI)

- Health information that is created or received by Rayaf Health and its affiliated practices which relates to the past, present, or future physical or mental health or condition of a patient;
- The provision of health care to the patient; **or**
- The past, present, or future payment for the provision of health care to the patient, *if* that information either identifies the patient *or* there is a reasonable basis to believe the information can be used to identify the patient ***and***
- Is transmitted or maintained in any form or medium in a designated record set.

## De-identification

- The removal of certain elements of PHI so that the information no longer identifies a particular individual. Once de-identified, this information is no longer considered PHI and can be used without regard to privacy rules.

## Disclosure of PHI

- The release, transfer, provision of, access to, or divulging in any other manner, information to entities *outside* Rayaf Health.

## Use of PHI

- Means sharing, employment, application, utilization, examination or analysis of such information *within* Rayaf Health.

## Treatment

- Means the provision, coordination, or management of health care and related services, including coordination of care, consultations, and referrals.

## Payment

- Means activities undertaken by Rayaf Health:
    - To obtain premiums or determine coverage and benefits to obtain or provide reimbursement, and related activities such as determining individual eligibility, adjudication or subrogation of claims;
    - For billing, claims management, collection activities and related health care data processing;
    - For medical necessity and utilization review; and
    - Disclosure of certain information to consumer reporting agencies.

## Health Care Operations

- Generally includes:
    - Quality assessment, the development of protocols, and case management;
    - Quality assurance, review of the competence or qualifications of health care professionals;
    - Underwriting and premium ratings;
    - Medical review, legal services and auditing functions, including fraud and abuse detection compliance programs;
    - Business planning and development; business management; and
    - General administrative activities including:
        - compliance with HIPAA;
        - customer service;
        - resolving internal grievances;
        - due diligence in connection with a sale or transfer of a Rayaf Health entity,
        - the creation of “de-identified” health information, and
    - Training programs in which practitioners in areas of health care learn under supervision to practice or improve their skills.

# Requirements and Obligations

## Use or Disclosure of PHI

Rayaf Health may use and disclose PHI for treatment, payment and other health care operations of Rayaf Health.

Rayaf Health also may disclose PHI to other health care providers for their treatment and payment activities. However, Rayaf Health may only disclose PHI to other providers for their health care operation activities that are related to the following:

- Fraud and abuse detection and compliance activities; or
- Quality or competency assurance activities.

As a general rule, Rayaf Health will not use or disclose PHI for purposes other than treatment, payment, and health care operations without written authorization from the authorized individual (the patient's parent, guardian or representative or from the patient per state per federal and state privacy laws for minors).

## PHI Disclosure Tracking

Disclosures for purposes other than treatment, payment and health care operations shall be tracked unless they are made pursuant to an authorization.

Business Associates of Rayaf Health will be required to sign a Business Associate Agreement (BAA) and provide a patient, upon request, accounting of all such disclosures for the term outlined in the BAA.

## PHI Disclosure Tracking Form

The PHI disclosure tracking form will include the following elements:

- Date of each disclosure;
- Name and address of each organization or person who received the PHI;
- A brief description of the information disclosed; and
- Purpose for which the PHI was disclosed.

## Disclosures Requiring Tracking

Disclosures which require tracking are as follows:

- Rayaf Health team members who are victims of crime;
- Health oversight activities, such as those conducted by the Departments of Public Health;
- Judicial and administrative proceedings;
- Law enforcement purposes;
- Aversion of serious threat to health or safety;
- Worker's compensation; and
- Victims of abuse, neglect or domestic violence.

Inappropriate or unintentional disclosures must also be reported and tracked. Examples include:

- A Rayaf Health Associate sharing PHI about a patient in a conversation with a mutual friend not involved in the patient's care;
- The theft of patient files (hard copies or electronic) by an unknown third party; and
- The accidental transmission of PHI to an incorrect email or fax number.

Inappropriate and unintended disclosures must be reported to the Rayaf Health Privacy and Security Officer.

## Data Extractions- Research

Rayaf Health may use and disclose information as part of research studies. All such disclosures must be approved in accordance with the "Rayaf Health Instructions for Initiating a Clinical Study."

It is Rayaf Health's policy to de-identify this information whenever possible. Information that has been de-identified according to the guidelines below can be used without authorization or tracking.

## Guidelines for De-Identification

In order for information to be considered de-identified, all of the following data elements must be removed:

- Name
- Geographical subdivisions smaller than a state, except for the initial 3 digits of the zip code
- The month and day portions of dates relating to a patient. Examples
    - Date of birth
    - Date of service
    - Admission and discharge dates
- Telephone number
- Fax number
- E-mail address
- Social security number
- Medical record number
- Health plan beneficiary number
- Account number
- Certificate number
- License number
- Vehicle identifiers and serial numbers
- Device identifiers and serial numbers
- Web universal locators
- Internet protocol address numbers
- Biometric identifiers, e.g., fingerprint, voice, full face photo
- Any other unique identifying number, characteristic or code

## Limited Data Sets

If information is being used for research, public health or health care operations of the recipient, the limited data sets may include certain indirect identifiers such as admission and discharge dates, service dates, date of birth and death and zip codes.

The information will not include direct identifiers such as:

- Name
- Street address
- Telephone and fax numbers
- E-mail address
- Social security number
- Certificate/license numbers
- Vehicle identifiers and serial numbers
- URL and IP addresses
- Biometric identifiers including finger and voice prints and full face photos
- Medical record number
- Health plan beneficiary numbers
- Device identifiers and serial numbers

If limited data sets are used that contain any of the acceptable indirect identifiers, a data use agreement must be obtained from the recipients of the data.

## Data Use Agreements

The need for Data Use Agreements will be determined by the Rayaf Health Director of Research and Development, with input from the Rayaf Health Privacy and Security Officer and/or Law Department. Data Use Agreements will be the responsibility of the data extract business owner or the Rayaf Health Director of Research and Development.

Data Use Agreements will include:

- Permitted uses and disclosures consistent with the purposes of research, public health or health care operations of the recipient;
- Limitations on who can use or receive the data; and
- Agreement by the recipient not to re-identify the data or contact the patients.

## Minimum Necessary

Rayaf Health will make all reasonable efforts not to use or disclose more than the minimum necessary amount of PHI necessary to accomplish the intended purpose of the use or disclosure.

Rayaf Health may rely upon requests as being the minimum necessary PHI when requested from:

- A public official;
- A professional (such as an attorney, consultant or accountant who is Rayaf Health's business associate) seeking the information to provide services on our behalf; or
- A researcher.

The minimum necessary requirement is not imposed in any of the following circumstances:

- Disclosure to or a request by a health care provider for the purpose of treatment;
- Disclosure to an individual who is the subject of the information, or the individual's personal representative;
- Use or disclosure made pursuant to an authorization;
- Disclosure to HHS for complaint investigation, compliance review or enforcement;
- Use or disclosure that is required by law; or
- Use or disclosure made consistent with the HIPAA Electronic Transactions and Code Sets Standards (for example, routine disclosures made for claims payment, eligibility or remittance purposes).

## Internal Use of PHI

An assessment of all PHI created, used, stored or manipulated by Rayaf Health has been made. Access to this PHI by Rayaf Health team members has been reviewed to ensure that access to PHI is permitted only when necessary. When feasible, safeguards such as system passwords will be in place to prevent unauthorized access to PHI. Changes to the Minimum Necessary Internal Use Guidelines must be approved by the Privacy and Security Officer.

All Rayaf Health team members are personally responsible for limiting their access to PHI to only that which is necessary to perform their assigned responsibilities and job functions.

## Safeguards

Rayaf Health will use all reasonable efforts to safeguard PHI from accidental or intentional use or disclosure that is a violation of the requirements of this policy, and to protect against the inadvertent disclosure of PHI to persons other than the intended recipient. The HIPAA regulations do not require specific safeguards but instead require covered entities to determine what is reasonable to protect PHI. It will be Rayaf Health's responsibility to determine reasonable safeguards in each specific situation. The following guidelines have been developed to help define reasonable measures that will assist in the safeguard of PHI and should be adhered to as much as possible:

- Log off computers whenever you leave your work area;
- Keep passwords secret;
- Password protection should be used whenever possible on all equipment used to store PHI such as PCs, handheld devices, etc.;
- All employee system passwords must be revoked upon termination of employment.
- Keep PHI paper records in a locked office, drawer or file when not in use;
- Do not discuss confidential information in situations when unauthorized persons may overhear you;

- Destroy PHI when no longer required for use or retention, in accordance with company record management policies;
- Ensure that electronically stored PHI is “erased” when equipment is recycled or discarded;
- Dispose of PHI properly to assure compliance with state laws and Rayaf Health document retention policies. Shredders or other secure means of disposal should be used to prevent unauthorized or inadvertent disclosures;
- Send faxes containing PHI only to secure machines in provider or payer offices;
- Double-check every fax number before hitting *Send;*
- If using pre-programmed fax numbers make sure you double-check these before saving. Pre-programmed numbers should also be checked periodically for changes;
- Avoid group distributions when faxing PHI;
- Confirmation should be made that the party requesting the faxed information is authorized to receive it. It may be necessary to call the location requesting the fax in order to validate that the recipient is an authorized person;
- Locate fax machines in an area where unauthorized persons cannot view incoming faxes;
- Always include a confidentiality disclaimer on the cover sheet of every fax that contains PHI. The following is an example of a confidentiality disclaimer that can be used on faxes or e-mails containing PHI:

  > CONFIDENTIALITY NOTICE: The documents accompanying this fax (e-mail) transmission may contain confidential and proprietary information intended only for use by the recipient named. If you are not the intended recipient or the employee or agency authorized to deliver this fax (e-mail) to the intended recipient, you are hereby notified that any unauthorized disclosure, copying, distribution or taking of action in reliance on the fax is strictly prohibited. If you have received this fax in error, please immediately notify the sender by telephone (number listed above) to arrange the return or destruction of the information and all copies.”
- Avoid using the “reply to all” function in e-mail containing PHI;
- E-mails that contain PHI should be classified as confidential to prevent forwarding;
- Always include a confidentiality disclaimer at the end of every e-mail containing PHI;
- Work areas that are open to the public should be organized to prevent inadvertent disclosures of PHI. For example, computer screens should be facing away from public view. Screen savers should be set to work at short intervals;
- Only voice messaging systems with password protection should be used for messages including PHI;
- Records that must be transported by team members should be returned to Rayaf Health premises as soon as possible and should be reasonably secured when not on Rayaf Health premises; and
- Always report immediately any incidents of inappropriate disclosure, lost records or other privacy concerns to your supervisor or to the Privacy and Security Officer.

# Accountability and Discipline

## Guidelines

Violation of this Privacy Policy and related policies and procedures is serious and will be dealt with in accordance with established corrective action policies as outlined (TBD). Depending on the nature of the violation, steps in the corrective action process may be skipped. In certain circumstances, a violation may lead to immediate termination of employment. In addition to corrective action by the Rayaf Health, HIPAA imposes potentially substantial civil monetary penalties upon violators and criminal penalties for knowingly obtaining or disclosing PHI in violation of HIPAA.

## Training

Rayaf Health provides privacy training for all personnel likely to have access to protected health information. Training will be required within TBD (X) days of hire for all team members. Rayaf Health will provide additional privacy training whenever privacy practices are materially altered. Upon completion of training, team members will sign an acknowledgment of training and agreement to comply with Rayaf Health policies. A copy will be kept in the Human Resources file for future audit. It is the Manager's responsibility to ensure completion of training and its documentation.

# Compliance Reviews

## Audits

Periodic internal audits will be performed to assess compliance to the Privacy Policy and other related policies and procedures. All team members are expected to cooperate with any Rayaf Health audit.

## Problem / Complaints

Resolution Process

When Rayaf Health team members are faced with a privacy concern or become aware of a planned, suspected or actual violation of the Privacy Policy or other related policies and procedures, they must take action or refer it to someone who can resolve it.

The following are steps to follow for suspected or actual violations:

- Identify the concern and the nature of the situation;
- Report the concern promptly to your supervisor or other Privacy and Security Officer; and
- Ensure that an appropriate solution is formulated using knowledge of this policy and other related policies and procedures. The plan of correction should be the joint effort of the individuals involved along with their manager(s) and the Privacy Officer and/or Law Department when necessary.

# Reporting of Suspected Violations of Privacy Practices

## Non-Retaliation and Internal Reporting

All team members, including supervisors and managers, have a responsibility to promptly report suspected violations of the Privacy Policy and other related policies and procedures. No employee may dismiss, ignore, or fail to report information giving rise to a suspected violation, even if obtained indirectly. Failure to report a suspected violation may subject the employee to disciplinary action, up to and including termination.

Team members who in good faith report a suspected privacy violation will not be subjected to retaliation or reprisal for the act of reporting. Reports should be made to a supervisor or other appropriate Company personnel. Team members cannot, however, exempt themselves from the consequences of personal wrongdoing by reporting their own misconduct. In such cases, self-reporting will be taken into account in determining the appropriate form of discipline but will not operate as a waiver of personal accountability.

In order to provide team members with a confidential way of reporting any concerns or questions that may arise as part of the Rayaf Health Code of Conduct. Rayaf Health has a confidential, toll-free Compliance Help-Line. The number for the Compliance Help-Line is (xxx) xxx-xxxx. The Compliance Help-Line is available 24 hours a day, 7 days a week. Any person calling the Compliance Help-Line will not be required to furnish his or her name, and calls are not traced or recorded. A professional employed by an outside company will answer the Compliance Help-Line and the caller will be asked a series of questions. The operator will document the information from the caller and submit a confidential and anonymous report of the information provided by the caller to the Compliance Officer. All calls to the Compliance Help-Line or submitted directly to the Compliance Officer are strictly confidential, and information from the call is provided only to those managers who have a need-to-know as required by the investigation or to implement appropriate remedial action. In addition, translation services in several languages are available upon request from the caller.

Any supervisor, manager, or employee who is found to have conducted or condoned retaliation in response to a good-faith report of a suspected privacy violation will be subject to discipline, up to and including termination.