General Privacy Policy

POLICY OWNER: Compliance and Practice Data Management

Effective Date: 01.01.2021

PURPOSE

To provide background information and direction to Futurhealth's workforce regarding Futurhealth's HIPAA policies.

POLICY

References to "Futurhealth" in these privacy policies shall refer to Futurhealth LLC, San Diego, CA, and any other affiliated professional corporations that are referenced in Futurhealth's Notice of Privacy Practices. It is the intent of Futurhealth to comply with all provisions of the Health Insurance Portability and Accountability Act ("HIPAA") as well as the Health Information Technology for Economic and Clinical Health ("HITECH") Act, and all regulations promulgated under such laws (collectively referred to herein as "HIPAA"). To that end, Futurhealth has created and implemented several written policies and procedures.

MINIMUM NECESSARY USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

When using or disclosing PHI, or when requesting PHI from another organization covered by HIPAA, reasonable efforts will be taken to limit the PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. This means, that to the extent practicable, the information contained in a Limited Data Set must be used, disclosed, or requested.

A. Limited Data Set is PHI that excludes direct identifiers of the individual or of relatives, employers, or household members of the individual. A Limited Data Set excludes all of the following:
    a. Names;

b. Address information, other than town or city, state, and zip code;
c. Telephone numbers;
d. Fax numbers;
e. E-mail addresses;
f. Social security numbers;
g. Medical record numbers;
h. Health plan beneficiary numbers;
i. Account numbers;
j. Certificate/license numbers;
k. Vehicle identifiers and serial numbers, including license plate numbers;
l. Device identifiers and serial numbers;
m. Web Universal Resource Locators (URLs);
n. Internet Protocol (IP) address numbers;
o. Biometric identifiers, including finger and voice prints; and
p. Full face photographic images.

B. If it is not practical to limit the information to a Limited Data Set, PHI beyond a Limited Data Set may be used, disclosed, or requested, as long as the PHI is limited to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

C. The minimum necessary standard DOES NOT apply to:
   a. Disclosures to or requests by healthcare providers for treatment;
   b. Disclosures to the individual who is the subject of the information;
   c. Uses or disclosures made in compliance with an authorization by the individual;
   d. Disclosures to the Department of Health and Human Services; and
   e. Uses or disclosures required by law.

D. The minimum necessary standard DOES apply to:
   a. Employees who access PHI in the performance of their duties;
   b. Requests for PHI from other organizations governed by HIPAA;
   c. Disclosures that occur on a recurring basis; and
   d. Uses or disclosures of PHI that fall outside the scope of section "C" above.

E. Unless a specific justification is given, requests for an entire medical record should not be granted.

F. You can rely on the judgment of the party requesting the disclosure to limit the amount of PHI to the minimum necessary when the request is made by:
    a. A public official;
    b. Another organization governed by HIPAA;
    c. A professional who is a workforce member or business associate of an organization governed by HIPAA and is seeking the information to provide services for that organization; and
    d. A researcher with appropriate documentation from an institutional review board or privacy board.
G. Disclosures made on a non-routine basis are reviewed individually to determine that the disclosure or the request is the minimum necessary to accomplish the purpose of the disclosure.
H. PHI may be used to verify an individual's identity.

USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION FOR MARKETING PURPOSES AND PROHIBITION OF THE SALE OF PHI

Marketing is a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. Marketing does not include a communication made: (i) face to face by a provider at Futurhealth to an individual; (ii) in the form of a promotional gift of nominal value by Futurhealth; (iii) to provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by Futurhealth in exchange for making the communication is reasonably related to Futurhealth's cost of making the communication; (iv) for the following treatment and health care operations purposes, except where Futurhealth receives financial remuneration in exchange for making the communication:

A. For treatment of an individual by a healthcare provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;
B. To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits

of, Futurhealth making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

C. For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

However, marketing does mean any communication from Futurhealth or a business associate of Futurhealth to a patient about a product or service that encourages the patient to purchase or use the product or service if Futurhealth receives financial remuneration from the other entity or its affiliate to make such a communication.

Financial remuneration means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual.

Futurhealth can only use PHI for marketing purposes if Futurhealth obtains an individual's authorization. The individual must authorize these marketing communications before they occur.

Futurhealth may not receive any financial remuneration in exchange for any PHI of an individual unless Futurhealth obtains an authorization from the individual which indicates that the individual's PHI can be exchanged for remuneration to the Futurhealth from the entity receiving the PHI. The following exceptions apply:

A. When the purpose of the exchange is for public health purposes pursuant to 45 CFR 164.512(b) or 45 CFR 164.514(e);
B. When the purpose of the exchange is for research purposes pursuant to 45 CFR 164.512(i) or 164.512(e), where the only remuneration received by Futurhealth is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purposes;
C. When the purpose of the exchange is for treatment and payment purposes pursuant to 45 CFR 164.506(a);
D. Where the purpose of the exchange is for the sale, transfer, merger, or consolidation of all or part of Futurhealth and for related due diligence

and pursuant to 45 CFR 164.506(a);

E. Where the exchange is to or by a business associate for activities that the business associate undertakes on behalf of Futurhealth, pursuant to 45 CFR 164.502(e) and 164.504(e), and the only remuneration provided is by Futurhealth to the business associate for the performance of such activities;
F. Where the exchange is to an individual when requested under 45 CFR 164.524 or 164.528;
G. Where the exchange is required by law as permitted under 45 CFR 164.512(a); and
H. Where the exchange is for any other purpose permitted by and in accordance with the applicable requirements of Subpart E of Part 164 of Title 45 of the Code of Regulations, where the only remuneration received by Futurhealth is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee otherwise expressly permitted by other law.

Any communication that could be construed as being marketing will be evaluated by the Privacy Officer prior to the communication being sent. Legal counsel may also evaluate these communications.

If it is determined that the communication falls within the definition of marketing, a patient's authorization will be obtained as required by 45 CFR 164.508.

No PHI may be provided to any third party in exchange for financial remuneration unless one of the exceptions listed above in Section D is applicable.

PRIVACY COMPLAINT PROCESS

All complaints regarding the privacy practices must be reported to the Privacy Officer. The Privacy Officer shall investigate all privacy-related complaints.

PROCEDURE

An individual who believes his/her privacy rights have been violated may file a complaint with the Privacy Officer of Futurhealth or with the United States

Secretary of the Department of Health and Human Services. Furthermore, all members of the workforce who believe that any HIPAA policies have been violated shall report such suspected violations to the Privacy Officer.

A. The Privacy Officer shall investigate all complaints in a timely manner. The investigation may include reviewing documents and conducting interviews of relevant witnesses. At the conclusion of the investigation, the Privacy Officer will prepare a written report which states the findings of the investigation and if there was a violation, any plan to address the violation. The Privacy Officer will then communicate that information in writing to the complaining party.

B. The Privacy Officer will maintain a log documenting the results of the investigation and resolution of all complaints.

C. Complaints may be submitted to the Privacy Officer via U.S. mail, fax, or e-mail:

    Mail: 1120 Rosecrans St, #297, San Diego CA, 92106
    E-mail: support@Futurhealthhealth.com

D. Individuals who wish to file a complaint with the Secretary of the Department of Health and Human Services must send their complaint to the Office of Civil Rights (OCR) headquarters:

    Office for Civil Rights
    U.S. Department of Health and Human Services
    200 Independence Avenue, S.W.
    Room 509F HHH Bldg. Washington,
    D.C. 20201

No person filing a complaint or providing information relevant to the investigation with the Privacy Officer or the OCR will be subject to retaliation or intimidation.

USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION FOR WHICH AN AUTHORIZATION IS REQUIRED

Protected health information (PHI) will not be used or disclosed without a written

authorization to do so from the individual or a person authorized to

act on behalf of the individual in making health care decisions unless HIPAA allows disclosure without an authorization. (See Policy Number 7: Uses and Disclosures of Protected Health Information For Which An Authorization Is Not Required).

PROCEDURE

A. A patient's authorization is required in all of the following situations:
    a. Prior to enrollment in a health plan, if necessary for determining eligibility;
    b. For the use and disclosure of psychotherapy notes unless:
        i. The psychotherapy notes are requested by the originator of the notes for treatment;
        ii. The notes will be used or disclosed for training in which students, trainees, or practitioners in mental health learn under supervision in group, joint, family, or individual counseling;
        iii. Futurhealth will use the notes to defend itself in a legal action brought by the individual;
        iv. The Department of Health and Human Services (HHS) will use the notes to investigate Futurhealth's compliance with HIPAA;
        v. The notes will be used to avert a serious imminent threat to the health or safety of a person or the public;
        vi. A health oversight agency will use the notes for a lawful oversight of the originator of the notes; or
        vii. A medical examiner or coroner will use the notes for their lawful activities.
    c. For disclosures to an employer for use in employment related determinations;
    d. For research purposes unrelated to the patient's treatment;
    e. For marketing;
    f. For the sale of protected health information; and
    g. For any situation in which a third party requests records or Futurhealth plans to disclose PHI and such disclosure is not permitted under Policy Number 7: Uses and Disclosures of Protected Health Information For Which An Authorization Is Not Required and Policy Number 18: Uses and Disclosures for Treatment, Payment and Health Care Operations.

USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION FOR WHICH AN AUTHORIZATION IS NOT REQUIRED

Protected health information (PHI) may be used or disclosed without the written authorization from the individual, and without providing notice to an individual only in very specific situations.

PROCEDURE

Futurhealth may use and disclose PHI without a patient authorization in all of the situations listed below. If you receive a request to release PHI outside of the organization and you are not typically involved in releasing such information you must contact the Privacy Officer before any PHI can be released.

A. In accordance with the Policy on Uses and Disclosures for Treatment, Payment and Health Care Operations.

B. When the use or disclosure is required by law and is limited to the relevant requirements of such law.

C. Disclosures for public health activities to:
    a. A public health authority that is authorized by law to collect, receive, or report such information for the purpose of preventing or controlling disease, injury or disability as well as to conduct public health surveillance, investigations, and interventions;
    b. A public health authority authorized by law to receive reports of child abuse or neglect;
    c. A person subject to the authority of the Food and Drug Administration (FDA) because that person is responsible for the quality, safety or effectiveness of a FDA-regulated product or activity. The purposes of these disclosures include:
        i. To collect or report adverse events, product defects, or biological product deviations;
        ii. To track FDA-regulated products;
        iii. To allow and notify individuals about product recalls, repairs, replacements, or lookbacks; or
        iv. To conduct post-market surveillance.
    d. A person who may have been exposed to or may be at risk of contracting or spreading a communicable disease or condition; or

e. An employer about an individual who is a member of the employer's workforce if:
    i. Futurhealth provides health care to the workforce member at the request of the employer to conduct an evaluation relating to medical surveillance of the workplace or to evaluate whether the individual has a work-related illness or injury;
    ii. The PHI that is disclosed contains findings that indicate a work-related illness or injury or workplace-related medical surveillance;
    iii. The employer needs such findings in order to comply with federal and state labor regulations which require the recording of work-related illnesses or injuries or the carrying out of responsibilities for workplace medical surveillance; and
    iv. Written notice of the disclosure is given to the individual at the time that health care is provided or by posting the notice prominently where the health care is provided, if the care is provided at the work site.
f. A school, about an individual who is a student or prospective student of the school, if:
    i. The PHI that is disclosed is limited to proof of immunization;
    ii. The school is required by state or other law to have such proof of immunization prior to admitting the individual; and
    iii. Futurhealth obtains and documents the agreement to the disclosure from either: a parent, guardian or other person acting in loco parentis of the individual, if the individual is an unemancipated minor; or the individual, if the individual is an adult or emancipated minor.

D. Disclosures about victims of abuse, neglect or domestic violence.
    a. PHI about an individual who is believed to be a victim of abuse, neglect, or domestic violence may be disclosed to a governmental authority, including a social or protective services agency:
        i. The disclosure must be limited to the extent required by law;
        ii. The individual must agree to the disclosure;
        iii. The disclosure must only be to the extent that is expressly authorized by statute or regulation; and
        iv. There is a belief that the disclosure is necessary to prevent serious harm to the individual or others; or

v. If the individual does not have the capacity to agree, a law enforcement, or other public official authorized to receive the report, represents that the PHI to be disclosed is not intended to be used against the individual and that an immediate enforcement activity that depends on disclosure would be significantly adversely affected by waiting until the individual is able to agree to the disclosure.

b. The individual must be promptly informed that the report concerning the suspected abuse, neglect, or domestic violence has been or will be made, except if:
    i. There is a reasonable belief that informing the individual would place the individual at risk of serious harm; or
    ii. The disclosure would be made to a personal representative and there is a reasonable belief that the personal representative is responsible for the abuse, neglect, or other injury.

E. Uses and disclosures for health oversight activities
    a. PHI may be disclosed to a health oversight agency for oversight activities authorized by law including audits, inspections, licensure, or disciplinary actions, or other activities necessary for the appropriate oversight of:
        i. The health care system;
        ii. Government benefit programs for which health information is relevant to beneficiary eligibility; or
        iii. Entities subject to government regulatory programs and civil rights laws for which health information is required to determine compliance.
    b. Health oversight activities do not include:
        i. An investigation or other activity in which the individual is the subject of the investigation;
        ii. An investigation or activity that is not related to:
            1. The receipt of health care;
            2. A claim for public health benefits; or
            3. Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for those benefits or services.

F. Disclosures for law enforcement purposes

a. PHI may be disclosed as required by laws that mandate the reporting of certain types of wounds or other physical injuries. The mandates may be in the form of:

i. A court order, court-ordered warrant, subpoena, or summons issued by a judicial officer;
ii. A grand jury subpoena; or
iii. An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:
    1. The information sought is relevant and significant to a legitimate law enforcement inquiry;
    2. The request is specific and limited to the extent reasonably practicable given the purpose for which the information is sought; and
    3. Information that cannot be linked to an individual could not reasonably be used.

b. PHI may be disclosed in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person.
    i. Only the following information may be disclosed for this purpose:
        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; and
        8. A description of distinguishing physical characteristics.
    ii. DNA, DNA analysis, dental records, typing, samples, or analysis of body fluids or tissue may not be disclosed.

c. PHI may be disclosed in response to a law enforcement official's request for such information about an individual who is a victim or is suspected to be a victim of a crime if:
    i. The individual agrees to the disclosure; or
    ii. The individual does not have the capacity to give their agreement provided that:
        1. The law enforcement officer represents a need for the information to determine whether a violation by a person other than the victim has occurred and such

information was not intended to be used against the victim;

2. The law enforcement official represents that immediate law enforcement activity depends on the disclosure and would be significantly and adversely

affected by waiting until the individual is able to agree to the disclosure; and

3. The disclosure was determined to be in the best interest of the individual.

d. PHI may be disclosed to a law enforcement official about an individual who has died to alert law enforcement of the death if there is suspicion that the death is the result of criminal conduct.
e. PHI may be disclosed to a law enforcement official if there is a good faith belief that the information is evidence of criminal conduct that occurred on Futurhealth's premises.
f. PHI may be disclosed to a law enforcement official in response to a medical emergency on the premises and the disclosure appears necessary to alert law enforcement to:
    i. The commission or nature of a crime, except for abuse, neglect, or domestic violence which is subject to section "C";
    ii. The location or victim(s) of such crime; or
    iii. The identity, description, and location of the perpetrator of such crime.

G. Uses and disclosures about decedents

a. PHI may be disclosed to coroners, medical examiners, and funeral directors to carry out their duties.
b. Disclosures made to funeral directors include those made in reasonable anticipation of the individual's death.
c. PHI may be disclosed to a family member, other relative, or close personal friend if such person was involved in the deceased's care or payment for health care prior to decedent's death, if the PHI is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the decedent that is known to Futurhealth.

H. Uses and disclosures for cadaveric organ, eye or tissue donation purposes

a. PHI may be disclosed to an organ procurement organization to facilitate organ, eye or tissue donation and transplantation.

I. Uses and disclosures for research purposes

a. PHI may be disclosed for research purposes only in accordance with 45 C.F.R. 164.512(i).

J. Uses and disclosures to avert a serious threat to health or safety

a. PHI may be used or disclosed if there:

i. Is a good faith belief that the use or disclosure is necessary, and is to a person who is reasonably able, to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; or
ii. Is necessary for law enforcement authorities to identify or apprehend an individual who made a statement admitting participation in a violent crime that may have caused serious physical harm to the victim.

b. Disclosure may not be made if:
i. The information to be disclosed was discovered during treatment to mitigate the propensity to commit the criminal conduct that is the basis for the disclosure, such as counseling or therapy; or
ii. Through the request by the individual to initiate or to be referred for the treatment.

c. The information to be disclosed is limited to:
i. The statement of the individual who is believed to have participated in a violent crime that may have caused serious harm to the victim;
ii. Name and address;
iii. Date and place of birth;
iv. Social security number;
v. ABO blood type and Rh factor;
vi. Type of injury;
vii. Date and time of treatment;
viii. Date and time of death, if applicable; and
ix. A description of distinguishing physical characteristics.

d. If PHI is used or disclosed in accordance with section "I" then there is a presumption that the use or disclosure was done in good faith and based on actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

K. Uses and disclosures for specialized government functions

a. PHI may be used or disclosed for military and veterans activities.

b. PHI may be used by or disclosed to Armed Services personnel or foreign military personnel for activities deemed necessary by military command authorities to assure the proper execution of the military mission.

c. PHI may be disclosed to federal officials for lawful intelligence, counter-intelligence, and other national security activities.
d. PHI may be disclosed to federal officials for the protective services of the President or foreign heads of state.

e. PHI may be disclosed to a correctional institution or a law enforcement official who has lawful custody of an inmate if such PHI is necessary for:
    i. Providing health care to such individual;
    ii. The health and safety of such individual or other inmates;
    iii. The health and safety of the officers or employees of or others at the correctional institution;
    iv. The health and safety of those responsible for transporting inmates;
    v. Law enforcement on the premises of the correctional institution; and
    vi. The administration and maintenance of the safety, security, and good order of the correctional institution.

L. Disclosures for workers' compensation
    a. To the extent necessary, PHI may be disclosed to comply with laws relating to workers' compensation or other similar programs, that provide benefits for work-related injuries or illnesses, without regard to fault.

BREACH OF UNSECURED PROTECTED HEALTH INFORMATION

There will be an immediate investigation of all situations that might involve a Breach of unsecured protected health information (PHI). If a Breach has occurred, notification will be provided to all affected individuals, the Department of Health and Human Services (HHS), and if applicable, the media, in accordance with this policy.

PROCEDURE

A. Overview of the Reporting Requirements:
    a. Futurhealth must notify an individual if: (1) the individual's unsecured PHI was accessed, used or disclosed in a way not allowed under the HIPAA privacy rule; and (2) Futurhealth cannot demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment which includes the factors noted in this Policy below. Futurhealth is under a strict deadline for giving notice of Breach to an individual. Therefore, if a member of

Futurhealth's workforce, or an agent of Futurhealth

knows or even suspects that an individual's PHI has been used, disclosed, accessed or obtained in a way that is not allowed under HIPAA, he or she must immediately report this information to the Privacy Officer. The Privacy Officer will determine whether HIPAA requires notice to the individual, and if notice is required, the Privacy Officer will arrange for the notice to be provided.

B. Definitions

a. Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA privacy rule, which compromises the security or privacy of the PHI. Unless an exception listed in Paragraph 4(b) of this Policy applies, the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA privacy rule is presumed to be a Breach unless Futurhealth can demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

   i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
   ii. The unauthorized person who used the PHI or to whom the disclosure was made;
   iii. Whether the PHI was actually acquired or viewed; and
   iv. The extent to which the risk to the PHI has been mitigated.

b. Unsecured PHI means PHI that has not been rendered unusable, unreadable or indecipherable to persons who are not authorized to access it, by encryption in accordance with valid encryption processes recognized by the following National Institute for Standards and Technology ("NIST") standards:

   i. Data at rest - NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.
   ii. Data in motion - 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

With respect to discarded data, paper, film and other hard copy documents, such documents must have been discarded by shredding or complete destruction such as burning or pulverizing.

Redaction is not acceptable. Electronic media must have been destroyed by clearing, purging or destruction in

accordance with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the PHI cannot be retrieved.

C. Reporting of Suspected Breach
    a. Any member of the workforce or agent of Futurhealth who discovers a potential Breach shall report it to the Privacy Officer.
    b. Business associates shall be required to report a Breach to the Privacy Officer of Futurhealth. This requirement should be included in Futurhealth's Business Associate Agreement.
D. Investigation of Suspected Breach
    a. The Privacy Officer shall review the circumstances of the suspected Breach to determine: (1) whether any exception to the reporting rule applies; and (2) whether Futurhealth can demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment of at least the factors described in Section 2(a) of this Policy.
    b. Exceptions
        i. If PHI was acquired, accessed or used by a workforce member or agent of Futurhealth or a business associate, but the acquisition, access or use was made in good faith and within the scope of permitted activities of the workforce member/agent, and there is no further unpermitted use or disclosure, then this is not a Breach and no reporting is required.

            Example: A Futurhealth employee who has authority to access patient records in order to perform his work responsibilities mistakenly accessed the wrong patient record. When the employee realized the error, he closed the record and did not retain any information or further disclose any information.

        ii. If PHI was inadvertently disclosed by one workforce member or agent of Futurhealth or a business associate to another workforce member/agent, and there is no further unpermitted use or disclosure, then this does not constitute a Breach and no reporting is required.

iii. If PHI was disclosed, but Futurhealth or business associate believes in good faith that the unauthorized person to

whom the disclosure was made would not reasonably have been able to retain such information, the disclosure is not a Breach and no notification is required.

Example: A nurse mistakenly hands a patient the discharge paper of another patient. Before the patient leaves, the nurse realizes the mistake and retrieves the paper from the patient.

iv. If the PHI was disclosed to or available for access by an unauthorized person, but the information was encrypted according to the standards identified in Section 2(b) of this Policy, there is no Breach and notification is not required.

Example: An employee of Futurhealth leaves a laptop at the airport and subsequently the laptop cannot be found. The laptop contains PHI, but all such information is encrypted according to the standards in this Policy. Because the Breach does not involve "unsecured PHI" no notification is required.

c. Compromise

i. If none of the exceptions apply, the Privacy Officer should review the circumstances of the suspected Breach to determine if Futurhealth can demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment of at least the factors described in Section 2(a) of this Policy.

ii. In certain circumstances, Futurhealth may be able to eliminate or reduce the risk of compromising the PHI by entering into a confidentiality agreement with the recipient of the information wherein the recipient agrees to destroy the information or agrees that it will not further use or disclose the information.

iii. If the risk assessment results in a conclusion that Futurhealth cannot demonstrate that there is a low probability that the PHI has been compromised, Futurhealth must make notification to the Covered Entity as described below in Paragraph 5.

E. Breach Notification to Individuals

a. Written Notice to the Individual(s)

i. If notice is required following the investigation and analysis noted above in this Policy, Futurhealth should notify the individual in writing. All persons who are the subject of a Breach of unsecured PHI must be individually notified, regardless of the number of persons involved.

ii. Notification will be sent without unreasonable delay, but in no event later than 60 days after discovery of the Breach. EXCEPTION: If Futurhealth has been notified by a law enforcement official in writing that notification would impede a criminal investigation, notification will be delayed and the reason documented.

iii. Notice will be sent to the individual's last known address by first class mail. If the individual had agreed in advance to receive notice electronically, notice may be given by email.

iv. If Futurhealth knows the individual is deceased and has the address of the next of kin or personal representative of the individual, Futurhealth will send written notice by first class mail to either the next of kin or personal representative, as applicable. The notification maybe provided in one or more mailings as information is available.

v. The notice will contain the following information:

1. A brief description of what happened;
2. A description of the types of unsecured PHI involved in the Breach;
3. Any steps the individual should take to protect him/herself from potential harm resulting from the Breach;
4. A brief description of steps Futurhealth is taking to investigate the Breach, to mitigate harm to individuals, and to protect against future Breaches; and
5. Contact procedures for the individual to ask questions, including a toll-free telephone number, an e-mail address, and Web site or postal address.

b. Substitute Notice to the Individual(s)

i. If contact information for the individual is out-of-date, substitute notice will be given in a way reasonably calculated to reach the individual.

ii. If there is insufficient contact information for ten or more individuals, then substitute notice will either be posted on the home page of Futurhealth's website, or notice will be conveyed through major print or broadcast media.

c. Urgent Notice to the Individual(s)

i. If there is danger of imminent misuse of the unsecured PHI, the individual will be notified by telephone or other means in addition to written notice.

F. Breach Notification by Publication

a. If a Breach of unsecured PHI involves 500 or more residents of the same state or any jurisdiction smaller than a state, such as a county or city, then in addition to notifying the affected individuals, Futurhealth should notify prominent media outlets in the state. In the notice, Futurhealth should provide all of the information that must be included in the individual notices.

G. Breach Notice to HHS

a. Immediate Notice. If a Breach of unsecured PHI involves 500 or more individuals, regardless of where they reside, Futurhealth should notify The Department of Health and Human Services ("HHS") of the breach at the same time notice is given to the individual individuals. Futurhealth should notify HHS through HHS' website, which can be found at http://hhs.gov/ocr/privacy/hipaa/administrative/index.html.

b. Annual Notice. For Breach incidents involving fewer than 500 individuals, Futurhealth must maintain a log of all breach incidents during the calendar year and report all breaches to HHS not later than 60 days after the end of each calendar year.

Note: The Breach notification requirements only apply to Breaches that occur on or after September 23, 2009. Therefore, if Futurhealth receives notice that a Breach of unsecured PHI occurred in 2008, and there has been no further Breach, Futurhealth is not required to notify individuals or HHS.

H. Documentation

a. Futurhealth shall maintain all documentation related to investigations of suspected and actual breaches for at least six (6) years after completion of the investigation.

RIGHT TO REQUEST CONFIDENTIAL COMMUNICATIONS AND TO RESTRICT ACCESS OR DISCLOSURE OF PROTECTED HEALTH INFORMATION

Any reasonable request for confidential communications of protected health information (PHI) must be accommodated. Individuals need not explain the reason for their request. However, the request must be reasonable, be made in writing, and specify an alternative address or method of contact.

All requests for restrictions on uses and disclosures will be considered by Futurhealth.

PROCEDURE

A. Confidential Communications
   a. Individuals have the right to request confidential communications of their PHI. All reasonable requests must be accommodated. Examples of types of communications to which this policy may apply include:
      i. Mailing or telephoning regarding appointment reminders;
      ii. Mailing bills or statements of payments due;
      iii. Sending test results; or
      iv. Prescription refill reminders.
   b. A reasonable accommodation may be conditioned on:
      i. Specification of an alternative address or method of contact; or
      ii. How payment will be handled, if applicable.
   c. The individual must not be required to explain the basis for the request as a condition of providing the communications, unless Futurhealth is a health plan, see subsection f, below.
   d. Requests for confidential communication must be made in writing.
   e. The patient's request for confidential communication must be documented in the patient's medical and billing records, and the original copy of the request form must be placed in the patient's medical record.
   f. If Futurhealth is a health plan, a request may be required to contain

a statement that disclosure of all or part of the

information to which the request pertains could endanger the individual.

B. Restrictions to Access and Disclosures
    a. An individual must be permitted to request the restriction of uses and disclosures of their PHI. The following are the rights and obligations when reviewing these types of requests:
        i. Futurhealth is not required to agree to a restriction except for a request of an individual to restrict disclosure of PHI about the individual to a health plan if:
            1. The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and
            2. The PHI pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid Futurhealth in full.
        ii. If Futurhealth agrees to the restriction, then the PHI may not be used or disclosed in violation of the restriction agreement, except in situations where the information is needed to treat the patient in an emergency. If restricted PHI is disclosed for emergency treatment, Futurhealth must request that the provider to whom the PHI was disclosed not make any further disclosures.
        iii. An agreed upon restriction must be documented.
        iv. Futurhealth may terminate an agreed upon restriction if:
            1. The individual agrees to or requests the termination in writing;
            2. The individual orally agrees to the termination and the oral agreement is documented; or
            3. The individual is informed that the agreement to the restriction is terminated except that such termination is only effective with respect to PHI created or received after the individual has been informed.
    b. Some examples of possible requests for restriction of uses and disclosures include:
        i. Individual requests that PHI not be shared with an outside transcription service, since the individual knows that person.
        ii. Individual requests that a certain diagnosis be left off a claim form.
        iii. Individual requests that certain PHI not be shared with other

providers

c. The Privacy Officer will review each restriction request and consider the following criteria:

i. Would Futurhealth be able to provide or continue treatment if Futurhealth honor the request?
ii. Would Futurhealth be able to submit a valid claim if Futurhealth were to honor the request?
iii. How would our agreement impact operations?
iv. Would Futurhealth be able to enforce the restriction internally now and in the future?

ACCOUNTING OF DISCLOSURES

Disclosures for purposes other than treatment, payment and healthcare operations that are not specifically authorized by the patient shall be tracked. Futurhealth must act on the individual's request for accounting, no later than 60 days after receipt of the request.

PROCEDURE

A. An individual has the right to receive an accounting of disclosures of protected health information (PHI) in the six years prior to the date on which the accounting is requested unless the disclosure was:
    a. To carry out treatment, payment and health care operations;
    b. To individuals of PHI about them;
    c. Incident to use or disclosure otherwise permitted by this policy;
    d. The type of PHI for which authorization is required according to Policy Number 6: Uses and Disclosures of Protected Health Information For Which An Authorization Is Required.
    e. For persons involved in the individual's care or other notification purposes
    f. For national security or intelligence purposes;
    g. To correctional institutions or law enforcement officials;
    h. Part of a Limited Data Set; or
    i. Made prior to the compliance date.
B. A Limited Data Set is PHI that excludes direct identifiers of the individual or of relatives, employers, or household members of the individual. A Limited Data Set excludes all of the following:
    a. Names;
    b. Address information, other than town or city, state, and zip code;

c. Telephone numbers;
d. Fax numbers;
e. E-mail addresses;
f. Social security numbers;

g. Medical record numbers;
h. Health plan beneficiary numbers;
i. Account numbers;
j. Certificate/license numbers;
k. Vehicle identifiers and serial numbers, including license plate numbers;
l. Device identifiers and serial numbers;
m. Web Universal Resource Locators (URLs);
n. Internet Protocol (IP) address numbers;
o. Biometric identifiers, including finger and voice prints; and
p. Full face photographic images.

C. Suspension of right to receive an accounting of disclosures

a. An individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official must be temporarily suspended for the time specified by such agency or official, if such agency or official
    i. Provides Futurhealth with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities
    ii. Specifies the time for which such a suspension is required.
b. If the statement is made orally then Futurhealth must:
    i. Document the statement, including the identity of the agency or official making the statement;
    ii. Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and
    iii. Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

D. Content of the Accounting

a. The accounting of disclosures of PHI must include:
    i. Date of the disclosure;
    ii. Description of information disclosed;
    iii. Name of party who received the PHI and, if known, the address of such party; and
    iv. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure;

E. If during the period covered by the accounting, disclosures were made for a particular research purpose to fifty (50) or more individuals, the accounting may provide:
    a. The name of the protocol or other research activity;
    b. A description in plain language of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;

c. A brief description of the type of PHI that was disclosed;
d. The date or period of time during which such disclosures occurred or may have occurred including the date of the last disclosure during the accounting period;
e. The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and
f. A statement that the PHI of the individual may or may not have been disclosed for a particular protocol or other research activity.

F. Responding to a Request for Disclosure:
    a. The requesting party will receive the accounting in writing from the Privacy Officer within 60 days. If additional time is required in order to comply with the request, an additional 30 days may be taken so long as the requesting party is notified in writing of the extension.
    b. The first accounting to an individual in any twelve (12) month period must be provided without charge. A [reasonable] fee will be imposed for each subsequent request for an accounting by the same individual within that twelve (12) month period.
G. An individual may request an accounting of disclosures for a period of time less than six (6) years from the date of the request.
H. All requests by individuals for an accounting of disclosures of PHI must be directed to the Privacy Officer at:

    Luke Mahoney
    Privacy Officer
    1220 Rosecrans St
    San Diego, CA 92106
    support@Futurhealthhealth.com

AMENDMENT OF PROTECTED HEALTH INFORMATION

An individual's protected health information (PHI) in a Designated Record Set will be amended at the request of the individual, in accordance with HIPAA requirements.

PROCEDURE

A. This policy applies to PHI that is part of a Designated Record Set. A Designated Record Set includes:

a. Medical records and billing records;
b. Enrollment, payment, claims and case or medical management records; and
c. Any records used to make decisions about the individual.

B. Requests for amendments must be submitted in writing to the Privacy Officer.
C. Futurhealth will respond to an individual's request for an amendment within 60 days after receipt of the request. If this is not possible, the individual will be given a written notice explaining the reasons for the delay and the date when the amendment will be completed. This extension will not go beyond thirty (30) days.
D. If Futurhealth accepts the individual's request for an amendment to PHI, Futurhealth will:
    a. Make the requested amendments;
    b. Inform the individual of the acceptance in a timely manner;
    c. Notify the people authorized by the individual that the amendments have been made and provide copies of the amendments as requested; and
    d. Notify business associates that the amendments have been made and provide copies upon request.
E. Denials
    a. An individual's request for amendment to PHI may be denied if it is determined that the PHI or record requested:
        i. Was not created by Futurhealth, unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;
        ii. Is not part of a Designated Record Set;
        iii. Is not available for inspection under HIPAA; or
        iv. Is accurate and complete.
    b. Following a denial to the individual's request for an amendment to PHI Futurhealth will notify the individual in plain writing of the denial which will include:
        i. The reason for denial;
        ii. Information about how the individual may submit a written statement concerning their disagreement with the denial;
        iii. A statement that, if the individual does not submit a statement of disagreement, the individual may request that Futurhealth provide the individual's request for amendment and the denial with all future disclosures of the PHI that is the

subject of the amendment; and

iv. A description of how the individual may file a complaint with Futurhealth or to the Secretary of Health and Human

Services. The description must include the name, or title, and telephone number of the Privacy Officer.

c. An individual is permitted to submit a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The length of this statement may be limited.
d. The individual's record or PHI that is the subject of the disputed amendment must be identified and linked to the individual's request for an amendment, the denial of the request, the individual's statement of disagreement, and any rebuttal in response to the statement of disagreement.
e. If a statement of disagreement has been submitted by the individual, then all future disclosures of PHI which concern the disagreement must include the individual's request for an amendment, the denial of the request, the individual's statement of disagreement, and any rebuttal in response to the statement of disagreement in full or a summary of such information.
f. If the individual has not submitted a written statement of disagreement, then the individual's request for amendment and the denial to that request, or an accurate summary of such information, will be included with any subsequent disclosure of PHI only if the individual has requested such action.

F. If informed by another health plan, health care clearinghouse, or health care provider of an amendment to an individual's PHI, Futurhealth will also amend the PHI of the individual within its system.
G. The titles of the persons or offices responsible for receiving and processing requests for amendments by individuals will be recorded.

RIGHT TO REQUEST ACCESS TO PROTECTED HEALTH INFORMATION

An individual has the right to request access to his or her own protected health information (PHI) in a designated record set.

PROCEDURE

A. A designated record set includes:
    a. Medical records and billing records;
    b. Enrollment, payment, claims and case or medical management records; and

c. Any records used to make decisions about the individual.

B. This right of access does not apply to:

a. Psychotherapy notes; and

b. Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

C. Requesting Access

a. Futurhealth shall provide the attached form for all individuals who request access to PHI.
b. The request shall be submitted and processed by the Privacy Officer.

D. Denying an individual's request to access their PHI:

a. If an individual's request for access to PHI is denied then Futurhealth will comply with the following requirements:
    i. Access will be given to any other PHI requested after excluding the denied PHI; and
    ii. A timely written denial will be given to the individual that is in plain language and includes:
        1. The reason for the denial of access;
        2. Any right of review (if applicable);
        3. How to file a complaint;
        4. The name and number of the person to whom the complaint may be filed; and
        5. The address of the United States Secretary of Health and Human Services.
b. An individual's request for access to PHI may be denied without providing the individual an opportunity for review of that denial in the following circumstances:
    i. The right of access to the PHI does not apply as explained by section "B";
    ii. The care was provided by or under the guidance of a correctional institution, the individual requesting PHI is an inmate, and obtaining such a copy may jeopardize the health, safety, or rehabilitation of the individual, other inmates, or other people at the correctional institution;
    iii. The PHI was collected during the course of research for treatment of the individual and the individual agreed to suspend his or her right of access during this period; and
    iv. The PHI was obtained from someone other than a health care provider under a promise of confidentiality and the access requested is reasonably likely to reveal the source of the information.
c. An individual's request for access to PHI may be denied with a right to have the denial reviewed. This review must be done by a health

care professional who did not participate in the original denial. The right to have a denial reviewed is allowed in the following circumstances:

i. A licensed health care professional determined that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
ii. The PHI makes reference to another person and a licensed health care professional determined that the access requested is reasonably likely to cause substantial harm to such other person; or
iii. The request for access is made by the individual's personal representative and a licensed healthcare professional determined that allowing access to the personal representative is reasonably likely to cause substantial harm to the individual or another person.

E. Allowing access to PHI.
   a. If an individual's request for access to PHI is accepted then:
      i. The individual must be provided with the access requested, including inspection or obtaining a copy, or both, of the PHI about the individual;
      ii. The PHI requested must be in the form and format requested by the individual;
      iii. A summary of the PHI may be provided in lieu of access to the PHI if the individual agrees in advance to such a summary and to any fees imposed; and
      iv. If the PHI that is the subject of a request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, Futurhealth must provide the individual with access to the PHI in the electronic form and format requested, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by Futurhealth and the individual.
   b. If an individual requests a copy of the PHI or agrees to a summary or explanation, a reasonable fee may be imposed provided that the fee includes only the cost of:
      i. Copying;
      ii. Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided in portable media;
      iii. Postage; or
      iv. Preparing an explanation or summary of the PHI if agreed to.

F. Futurhealth must respond to an individual's request for access to PHI no

later than thirty (30) days after receipt of the request. If action cannot be taken in response to the request to access PHI within the thirty (30) day limit then a thirty (30) day extension is allowed. Under these

circumstances, the individual must be given a written statement (within thirty (30) days of receipt of the request) of the reasons for the delay and the date by which action on the request will be completed. This extension may only be used once.

G. If an individual's request directs Futurhealth to transmit the copy of PHI directly to another person designated by the individual, Futurhealth must provide the copy to the person designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of PHI.
H. The following must be documented:
    a. The designated record sets that are subject to access by individuals; and
    b. The titles of the person or offices responsible for receiving and processing requests.

USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION TO PERSONAL REPRESENTATIVES

An individual's personal representative will be treated as the individual with respect to the individual's rights under HIPAA, for example, accounting of disclosures, amendment of PHI, and right to request access to PHI.

PROCEDURE

A. If under applicable state law a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making health care decisions, that person will be treated as the individual's personal representative and shall have all rights under HIPAA that the individual would have.
B. If the individual is an unemancipated minor, his or her personal representative is a parent or guardian with legal authority to make health care decisions on behalf of the minor. There are three circumstances in which the parent is not the personal representative with respect to the minor's PHI:
    a. When state or other law does not require the consent of another to perform the health care service given to the minor, the minor consents to the health care service, and the minor has not requested that such other person be treated as the personal representative;

b. When a court determines that the minor may obtain the health care service without the consent of a parent or guardian; and

c. When a parent agrees to a confidential relationship between the minor and the physician.

C. State or other law supersedes the access or lack thereof that a parent or guardian has to an unemancipated minor's PHI.
D. If the individual is deceased, the personal representative is the person with the legal authority to act on behalf of the decedent or the estate of the decedent. Futurhealth shall request reasonable documentation to verify that the personal representative has such legal authority – for example, a court order.
E. Futurhealth may not treat a person as the personal representative if there is a reasonable belief that the individual is being subjected to domestic violence, abuse or neglect by the personal representative or that treating such person as the individual's personal representative would endanger the individual and Futurhealth concludes that it is not in the best interest of the individual to treat the person as the individual's personal representative.

USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION REGARDING DECEASED INDIVIDUALS

The protected health information (PHI) of deceased individuals is subject to the same standards of use and disclosure as applies to the PHI of living individuals for fifty (50) years following the death of the individual.

PROCEDURE

A. A person who has the authority under the law to act on behalf of the deceased individual or for their estate will be treated as the decedent's personal representative for the purpose of using or disclosing the decedent's PHI.
B. Disclosures of PHI to medical examiners, coroners, and funeral directors to carry out their official duties are allowed.
C. Disclosure requests from a health provider for the purpose of treating a surviving relative of the deceased are allowed.
D. Disclosure requests from a public health authority that is legally authorized to receive such a report is allowed.
E. Disclosure requests from a researcher must include an oral or written certification that the use or disclosure is for research purposes using the PHI of the deceased, that the disclosure is necessary for the research,

and documentation of the death of the individual whose PHI is sought must be provided.

F. Disclosure of PHI may be made regarding an individual after the period of fifty (50) years following the death of the individual.
G. PHI of a deceased may be disclosed to a family member, other relative, or close personal friend who does not qualify as a personal representative in Section A above, if such person was involved in the deceased's care or payment for health care prior to decedent's death, if the PHI is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the decedent that is known to Futurhealth.

USES AND DISCLOSURES FOR TREATMENT, PAYMENT, AND HEALTH CARE OPERATIONS

Protected health information (PHI) may be used or disclosed without a patient authorization for purposes of treatment, payment, or health care operations as specifically provided in this policy.

PROCEDURE

A. Definitions:
    a. *Health care operations* means any of the following activities of Futurhealth:
        i. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
        ii. (2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of

non-health care professionals, accreditation, certification, licensing, or credentialing activities;

iii. (3) Except as prohibited under Section 164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities related to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of 45 CFR 164.514(g) are met, if applicable;

iv. (4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

v. (5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

vi. (6) Business management and general administrative activities of Futurhealth, including, but not limited to:

1. (i) Management activities relating to implementation of and compliance with the requirements of HIPAA;
2. (ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that PHI is not disclosed to such policy holder, plan sponsor, or customer;
3. (iii) Resolution of internal grievances;
4. (iv) The sale, transfer, merger, or consolidation of all or part of Futurhealth with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and
5. (v) Consistent with the applicable requirements of 45 CFR 164.514, creating deidentified health information or a limited data set, and fundraising for the benefit of the covered entity.

b. *Payment* means:

i. The activities undertaken by:

1. A health plan to obtain premiums or to determine or

fulfill its responsibility for coverage and provision of benefits under the health plan (except as prohibited under Section 164.502(a)(5)(i); or

2. A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

ii. The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:

1. Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
2. Risk adjusting amounts due based on enrollee health status and demographic characteristics;
3. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
4. Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
5. Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and
6. Disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement:
    a. Name and address;
    b. Date of birth;
    c. Social security number;
    d. Payment history;
    e. Account number; and
    f. Name and address of the health care provider and/or health plan.

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

B. Except with respect to uses or disclosures that require an authorization

under 45 CFR 164.508(a)(2) through (4) or that are prohibited under 45 CFR 164.502(a)(5)(i), Futurhealth may use or disclose PHI for treatment, payment, or health care operations, as follows (provided such use or

disclosure is consistent with other applicable requirements of the Privacy Rule):

a. Futurhealth may use or disclose PHI for its own treatment, payment, or health care operations.
b. PHI may be disclosed for the treatment activities of another health care provider.
c. PHI may be disclosed to another health care provider, clearinghouse, or health plan for the payment activities of the entity that receives the PHI.
d. PHI may be disclosed to another health care provider, clearinghouse, or health plan for health care operations activities of the entity that receives the PHI, if both Futurhealth and receiving entity have or had a relationship with the individual who is the subject of the PHI being requested, the PHI pertains to such relationship, and the disclosure is:
    i. For a purpose listed in paragraph (1) or (2) of the definition of Health Care Operations under this policy; or
    ii. For the purpose of health care fraud and abuse detection or compliance.
e. PHI about an individual may be disclosed to another health care provider, clearinghouse, or health plan that participates in an organized health care arrangement if Futurhealth also participates in an organized health care arrangement and the disclosure is for any health care operations activities of the organized health care arrangement.

USES AND DISCLOSURES REQUIRING AGREEMENT OR OBJECTION

The Privacy Regulations allow use and disclose of protected health information ("PHI") for certain purposes, provided that, except in emergency situations, such use or disclosure is consistent with the individual's agreement or the individual's failure to object after being given an opportunity to do so.

PROCEDURE

A. Futurhealth may disclose to a family member, other relative, or any other person identified by the individual, the PHI directly relevant to such person's involvement with the individual's care or payment related to the individual's health care.

B. Futurhealth may use or disclose PHI to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual, of the individual's location, general condition, or death. Any such use or disclosure of PHI for such notification purposes must be in accordance with Paragraphs 3, 4 and 5 below, as applicable.

C. If the individual is present for, or otherwise available prior to, a use or disclosure permitted by Paragraphs 1 or 2 above and has the capacity to make health-care decisions, Futurhealth may use or disclose the PHI if Futurhealth:
    a. obtains the individual's agreement;
    b. provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or
    c. reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure.

D. If the individual is not present, or the opportunity to agree or object to the use or disclosure permitted by Paragraphs 1 or 2 cannot practicably be provided because of the individual's incapacity or an emergency circumstance, Futurhealth may, in the exercise of professional judgment, determine whether the disclosure is in the best interest of the individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with the individual's health care, including payment. Futurhealth may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of PHI.

E. Futurhealth may use or disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by Paragraph 2 of this Policy. The requirements in Paragraphs 3 and 4 above apply to such uses and disclosure to the extent that Futurhealth, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

F. If an individual is deceased, Futurhealth may disclose PHI of the individual to a family member, other relative, or close personal friend of

the individual, if such person(s) was involved in the individual's care or payment for health care prior to the individual's death, if the PHI is relevant to such person(s) involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to Futurhealth.

DISPOSAL OF PROTECTED HEALTH INFORMATION

Appropriate steps must be taken to dispose of any documents, film or hard copy materials that contain protected health information (PHI).

PROCEDURE

A. PHI in paper records, film or hard copy materials must be shredded, burned, pulped, or pulverized so that the PHI is rendered unreadable and otherwise cannot be reconstructed. Redaction is specifically prohibited as means of data destruction. In addition, documents cannot be disposed of in a public manner. For example, documents with PHI may not be placed in the regular trash or in a dumpster. If documents are stored pending destruction, for example in a shred bin, the storage device must be locked and otherwise secured.
B. Electronic media (discs, phones, thumb drives, hard drives, and copy machines) and all other ePHI must be disposed of in accordance with Futurhealth's Security Policy on Disposal of ePHI.
C. All workforce members must follow this disposal policy at all times

COOPERATION WITH HHS INVESTIGATIONS

Futurhealth will cooperate with the Secretary of the United States Department of Health and Human Services ("Secretary") if the Secretary investigates whether Futurhealth has complied with the HIPAA requirements.

PROCEDURE

A. If any member of the workforce of Futurhealth receives notice in any form that the Secretary is requesting information or documents from Futurhealth, the member shall immediately notify Futurhealth's Privacy Official and Security Official.
B. The Futurhealth Privacy Official and Security Officials shall be in charge of ensuring that Futurhealth and all employees comply with the requests of

the Secretary.

C. Futurhealth and all members of Futurhealth's workforce shall cooperate fully and in a timely manner with the Secretary during the investigation.
D. Futurhealth will permit access by the Secretary during normal business hours to Futurhealth's facilities, books, records, accounts, and other sources of information, including protected health information (PHI), that are pertinent to ascertaining compliance with the applicable administrative simplification provisions. If the Secretary determines that exigent circumstances exist, such as when documents may be hidden or destroyed, Futurhealth must permit access by the Secretary at any time and without notice.
E. If any information required of Futurhealth during an investigation is in the exclusive possession of any other agency, institution, or person and the other agency, institution, or person fails or refuses to furnish the information, Futurhealth must so certify and set forth what efforts Futurhealth has made to obtain the information.

DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION

The Privacy Regulations allow Futurhealth to de-identify protected health information ("PHI"). Futurhealth will comply with the HIPAA standard for de-identification.

PROCEDURE

A. Futurhealth may de-identify PHI as follows:
    a. a person with appropriate knowledge of, and experience with, generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:
        i. applying such principles and methods, 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 an individual who is a subject of the information; and
        ii. documents the methods and results of the analysis that justify such determination.
B. In the alternative, de-identified information may be created by removing the following identifiers of the individual, or of relatives, employers, or household members of the individual:
    a. names

b. all geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
    i. the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
    ii. the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000;
c. 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;
d. telephone numbers;
e. fax numbers;
f. electronic mail addresses;
g. social security numbers;
h. Medical record numbers;
i. health plan beneficiary numbers;
j. account numbers;
k. certificate/license numbers;
l. vehicle identifiers and serial numbers, including license plate numbers;
m. device identifiers and serial numbers;
n. web Universal Resource Locators (URLs);
o. internet Protocol (IP) address numbers;
p. biometric identifiers, including finger and voice prints;
q. full face photographic images and any comparable images; and
r. any other unique identifying number, characteristic, or code, except as permitted for purposes of re-identification.

C. Futurhealth may assign a code or other means of record identification to allow information that has been de-identified to be re-identified by Futurhealth, provided that:
    a. the code or other means of record identification is not derived from

or related to information about the individual and is not

otherwise capable of being translated so as to identify the individual; and

b. Futurhealth does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

FUNDRAISING

Futurhealth may use limited sets of PHI for the purpose of raising funds.

PROCEDURE

A. Futurhealth may use, or disclose to a business associate or to an institutionally related foundation, the following PHI for the purpose of raising funds for its own benefit, without an authorization:
    a. demographic information relating to an individual (name, address, other contact information, age, gender and date of birth);
    b. dates of health care provided to an individual;
    c. department of service information;
    d. treating physician;
    e. outcome information; and
    f. health insurance status.
B. Futurhealth may not use or disclose PHI for fundraising purposes as permitted by Section A. unless a statement that Futurhealth may contact an individual to raise funds for Futurhealth and that an individual has a right to opt out of receiving such communications is included in Futurhealth's Notice of Privacy Practices;
C. Futurhealth will include with each fundraising communication it sends to an individual a clear and conspicuous description of how the individual may opt out of receiving any further fundraising communications. The method to opt out may not cause the individual to incur an undue burden or more than a nominal cost. For example, providing a toll free phone number or email address is acceptable.
D. Futurhealth must ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications.
E. Futurhealth will not use PHI for any fundraising purposes other than those permitted in Section A unless Futurhealth obtains an authorization from the individual.

F. Futurhealth may not condition treatment or payment on the individual's choice whether or not to opt out of receiving fundraising

communications.

G. Futurhealth may provide an individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications

NOTICE OF PRIVACY PRACTICES

A. Futurhealth will provide notice to all individuals, through a Notice of Privacy Practices ("Notice"), as to the permitted uses and disclosures of their PHI.
B. The Notice will be provided to individuals and will comply with the provisions set forth below.
C. Futurhealth will provide a Notice:
    a. No later than the date of the first service delivery, including service delivered electronically, to individuals.
    b. In an emergency situation, as soon as reasonably practicable after the emergency situation.
D. Futurhealth will provide a Notice upon request.
E. Except in an emergency situation, Futurhealth will make a good faith effort to obtain a written acknowledgement of the receipt of the Notice, and if not obtained, Futurhealth should document its good faith efforts to obtain such acknowledgement and the reasons why the acknowledgement was not obtained.
F. Futurhealth will have the Notice available at all service delivery sites for individuals to request to take with them and will post the Notice in a clear and prominent location where it is reasonable to expect individuals seeking service to be able to read the Notice.
G. If Futurhealth maintains a web site, it will prominently post its Notice on the web site and make the Notice available electronically through the web site.
H. Futurhealth may provide the Notice to an individual by e-mail, if the individual agrees to electronic Notice and such agreement has not been withdrawn. If Futurhealth knows that the e-mail transmission has failed, a paper copy of the Notice will be provided to the individual. Provision of electronic Notice by Futurhealth will satisfy the provisions of this Policy when timely made.

I. The individual who is the recipient of an electronic Notice retains the right to obtain a paper copy of the Notice from Futurhealth upon

request. The procedure for requesting the paper copy shall be set forth in the Notice.

J. Futurhealth will provide the Notice to individuals in accordance with the implementation specifications set forth in this Policy.
K. Futurhealth will document compliance with the notice requirements, by retaining copies of the Notices issued by Futurhealth for six years from the date of the Notices' creation or the date when they last were in effect, whichever is later.
L. The contents of the Notice will comply with the requirements of HIPAA.

ADMINISTRATIVE, PHYSICAL AND TECHNICAL SAFEGUARDS TO PROTECT PHI

Futurhealth has in place the appropriate administrative, technical, and physical safeguards to protect the privacy of Protected Health Information ("PHI").

PROCEDURE

A. Before any member of Futurhealth's workforce shall be granted access to PHI, Futurhealth's Privacy Official shall review the member's job responsibilities and determine whether such member needs access to PHI to perform the member's job functions. Only members who require access to PHI to perform their job functions will be granted access to PHI. Furthermore, the member shall only have access to the minimum PHI that is necessary for the member to complete his or her job tasks. The Privacy Official shall document for each member the assessment and whether and to what extent access to PHI shall be granted. The Privacy Official shall review each member's assessment no less than twice each year and each time a member's job responsibilities change.
B. Each member of the workforce who has access to PHI is responsible for taking appropriate measures to protect the privacy of PHI, including but not limited to, those measures specified in this Policy.
C. Individuals shall comply at all times with Futurhealth's Minimum Necessary Policy.
D. An Individual should never access PHI unless he or she is authorized to do so.
E. Each individual should only use and disclose PHI as directed by the

individual's supervisor and/or Futurhealth's Privacy Official to perform the

individual's job responsibilities. If an individual receives a request to use or disclose PHI other than as directed by the individual's supervisor or Futurhealth's Privacy Official, the individual should contact the Privacy Official before such use or disclosure.

F. Paper documents containing PHI must be secured in a locked cabinet after business hours. Paper documents containing PHI must be secured in a locked cabinet during business hours if the documents are not in use. Keys to the cabinets will only be provided to the employees who are granted access to the documents and the Privacy Official.

G. Each individual is responsible for securing his or her physical space when using paper documents that contain PHI. This means, for example, that individuals who are not authorized to view the documents should not physically be able to view the documents.

H. If PHI will be faxed to Futurhealth, (a) the fax machine will be placed in a location where only authorized recipients of PHI will have access to the fax machine, or (b) the fax recipient will periodically check the fax machine to remove all faxes containing PHI.

I. If Futurhealth must fax documents containing PHI, such faxes can never be delivered to public places such as to a Kinkos. Faxes can only be sent directly to the business address of the specific authorized recipient.

J. Prior to faxing documents containing PHI, the individual must double check the correct fax number of the recipient. When routinely faxing to the same fax number; the fax number shall be programmed into the fax machine if possible.

K. All faxes containing PHI must contain the following statement: This facsimile, including any attachment(s), is for the sole use of the intended recipient(s) and contains confidential information. Any unauthorized review, use, disclosure or distribution is strictly prohibited. If you are not the intended recipient, please immediately contact the sender by phone.

L. If PHI is mailed, it must be mailed using a service which allows tracking such as Fed Ex. In addition, the PHI must be sealed within the envelope or outside packaging which instructs the recipient to only open the package if the recipient is the correct intended recipient. The package should include contact information for the recipient to report the receipt of unintended packages.

M. If PHI must be discussed over the phone each individual should take appropriate precautions such as using a land line and having the discussion in a private area.
N. All offices which contain PHI must be locked and secured after hours.
O. If paper containing PHI is on the office premise, visitors must be required to check in before entering the office and shall be escorted by a member of Futurhealth's workforce at all times to ensure that the visitor does not have access to PHI. Visitor check-in logs must be maintained.
P. All members of Futurhealth's workforce are prohibited from removing from the office paper materials that contain PHI. For example, an employee may not take papers containing PHI home to work on a project.
Q. Paper documents containing PHI must be disposed of in compliance with Futurhealth's Disposal Policy. Under no circumstance shall paper containing PHI be disposed of in the trash.
R. All members of Futurhealth's workforce must comply with the safeguards found in Futurhealth's Security policies regarding electronic PHI, for example, the proper use of passwords, logging off computers, and disposal of electronic media.

EXCEPTIONS

Requests for an exception to this Policy must be submitted to the IT Manager for approval.

VIOLATION AND ENFORCEMENT

Any known violations of this policy should be reported to the IT Manager. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.