

1. Uses and Disclosures of Protected Health Information

PURPOSE

This policy explains the process for using or disclosing Protected Health Information (PHI).

POLICY

1.1. CFBHN will recognize that PHI cannot be used or disclosed except as described in CFBHN's policies and procedures.
§164.502

1.2. CFBHN will recognize that uses and disclosures can be made to carryout treatment, payment, or health care operations (TPO).
§164.506

1.3. CFBHN will recognize that certain uses and disclosures may require patient authorization.
§164.508

1.4. CFBHN will recognize that certain uses and disclosures may require an opportunity for the patient to agree or to object.
§164.510

1.5. CFBHN will recognize that certain uses and disclosures do not require patient authorization, or an opportunity for the patient to agree or to object.
§164.512
§164.514(f) and (g)

PROCEDURES

CFBHN does not provide direct services to clients and as such does not store or collect records for persons receiving services from subcontractors under the contracts through CFBHN. In the event CFBHN receives a request for specific client information regarding treatment this request should be forwarded to the CFBHN Privacy Officer for review and response. In most cases the request for specific client information should be directed to the agency or agencies that have provided services. Providing the names of agencies to a requestor, may be considered confidential and should not be released to a third party without a signed release of information, is required by law or regulation, or the request is accompanied by a document permitting the release of such information.

CFBHN expects subcontractors to make disclosures of PHI following these guidelines. CFBHN does not make disclosures of PHI on behalf of subcontractors and will direct all requests for client information to the agency or agencies that provided the services. The disclosure of the

agencies may in and of itself be a disclosure of PHI and this should be directed to the Privacy Officer prior to releasing any PHI.

The QI Director is the designated Privacy Officer.

In every instance of use or disclosure of Protected Health Information (PHI), you must make judgments about the identity, role, authority and needs of the PHI user/recipient. Based upon these judgments, you must then define the type and amount of PHI the user/recipient will be able to have. In almost every instance, this means providing only the minimum PHI that is necessary for the user/recipient to perform their role with "limited data sets" and/or to "de-identified" data. And you must determine if patient approval is required before use and disclosure.

For the typical activities of CFBHN such as Treatment, Payment and Operations (TPO), judgments can be made up-front rather than on a case-by-case basis. These judgments will enable you to put in place standard practices, assurances and agreements that will allow a variety of CFBHN workforce members to perform these tasks without having to seek guidance in every instance. But for use or disclosure circumstances that are not typical (generally not related to TPO), judgments must be made about almost every request. Therefore, the Privacy Officer should be involved in all atypical uses and disclosures.

The Privacy Officer must appropriately record all unusual disclosures (not a part of TPO and are not disclosures to the patient). Documentation must include all of the following:

- Person or organization requesting the information;
- Purpose of the request for PHI;
- Date of request;
- Description of the PHI disclosed;
- Date of disclosure.

These procedures provide more information on what restrictions that are required regarding use and disclosure. Any time a disclosure is made, you must follow the verification requirements in Policy 5.0, Verification Requirements for use and disclosure of PHI.

Disclosure Related to Treatment, Payment and Operations

Use Among, and Disclosure to Workforce members
§164.514(d)(2)

The Privacy Officer must categorize CFBHN managers, workforce members, contractors, consultants and Business Associates (workers) by the Protected Health Information (PHI) they need to do their jobs. For instructions and more detailed information, see the policies and procedures on administrative actions and minimum necessary standards.

Disclosing to Patients
§164.524

In most cases, CFBHN will accommodate a patient's right to see or copy his or her information. However, there are circumstances where providing some or all of the

information is not appropriate, particularly when the patient's representative is making the request. See the Patient's Right to Health Care Information section of these Policies and Procedures about how to handle a patient's request for PHI.

In most cases the client requesting the information will be directed to the agency or agencies that provided the service(s) for that information.

Disclosing to Family Members or Friends Involved in Care
§164.510(b)

In most cases the family member or friends requesting the information will be directed to the agency or agencies that provided the service(s) for that information.

Discussing PHI with the Patient's Family or Friend

CFBHN may disclose PHI to a person (a family member, other relative, a close personal friend, or any other person identified by the patient) involved with a patient's care and/or payment for care. The PHI disclosure must be relevant to this person's involvement in the patient's care and consistent with the wishes of the patient. (See below about the presence and ability of the patient).

Finding and Notifying Family Members

You may use or disclose PHI necessary to identify and locate a family member or personal representative of the patient, and notify them of the location, general condition or death of the patient. Such disclosures must be consistent with the wishes of the patient (see below about the presence and ability of the patient).

When the Patient is Not Present or Able

If the patient is not present, or is incapacitated or cannot respond because of an emergency situation, disclose the PHI to another person (like a family member, close friend, representative) only when you believe, in your professional judgment that such a disclosure is in the best interest of the patient. Before choosing the family member or friend with whom to discuss the PHI, consider if the patient has made any previous request for restrictions on sharing his or her PHI, such as a requirement for confidential communications. (See the section in these Policies and Procedures on Patient's Right to Request Privacy Protection.) Also, consider potential harm that may result from the disclosure (if, for example, you suspect that the person you are speaking with is abusing the patient). The person to whom you disclose PHI should also be someone you would reasonably expect to be involved with the patient's health care. These judgments also apply when allowing someone other than the patient to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of PHI.

Disclosing Through a Facility Directory (Does not apply to CFBHN) Disclosure to Other Providers
§164.502(b)(1) and (2)(i), §164.506(c)(2-5), §164.514(d)(iii)(B)

In most cases providers requesting the information will be directed to the agency or agencies that provided the service(s) for the information.

If a request from another provider is not routine (for example, from a provider that CFBHN does not regularly work with), or if you have any concern about the legitimacy of the request, use the Provider Request for PHI form, involve the Privacy Officer, and follow the procedures below. Furthermore, make sure that the people requesting the information are who they claim to be and have the authority to receive the PHI. See the Verification Requirements section of these Policies and Procedures about how to do that.

When another health care provider requests a patient's PHI, ask the provider to state the reason for seeking the information.

For Treatment

If another provider is seeking PHI in order to treat a patient, you can provide any of the PHI without the patient's authorization except for psychotherapy notes (share psychotherapy notes only with patient authorization). This means you do not have to apply the minimum standard when providing PHI to another health care provider for treatment purposes.

For Payment, Operations, Fraud and Abuse Detection, and Compliance

If other providers seek PHI for reasons related to payment, operations, fraud and abuse detection, or compliance issues, ask them to confirm that they have or had a relationship with the patient. If they cannot confirm this, do not provide them any PHI. Also ask them to confirm that they are classified as a "covered entity" under HIPAA. This simply means that they are required to comply with HIPAA just like CFBHN. If they are not a covered entity, you will have to decide what PHI you will provide using the minimum necessary standard (see that section in these Policies and Procedures). If they are a "covered entity" ask them to describe the minimum necessary information needed to achieve their purposes. Because they are a "covered entity," you can rely upon their judgment about this, if it appears reasonable. You do not have to get a patient's authorization or consent, but are not prohibited from doing so.

For Marketing and Fundraising

CFBHN does not solicit or provide PHI for marketing and/or funding raising purposes.

Disclosure to Affiliates
164.504(d)

CFBHN can disclose PHI to another "covered entity" (organization that must comply with HIPAA like CFBHN) for the treatment, payment and operations as if CFBHN and this affiliate were one entity if they:

- Are under the common ownership or control; and
- Combine functions; and
- Both implement safeguards to ensure HIPAA rules as they apply to the functions they perform; and
- Document this arrangement through a business associates agreement or a Memorandum of Understanding or Memorandum of Agreement.

Disclosure to Other Members of Organized Health Care Arrangements (OHCA)
§164.506(c)(5)

If CFBHN is a member of an OHCA, it can disclose PHI to other members for any health care operations activities of the OHCA.

Business Associate Use and Disclosure
§164.502(e) and §164.504(e)(1)

CFBHN Business Associates (see glossary) can create, use and accept PHI from CFBHN without patient authorization or agreement, as long as the associate uses proper safeguards (just like the ones implemented by CFBHN). To assure that Business Associates will implement such safeguards, CFBHN must enter into agreements with the Business Associates which commit them to do so. See the section in these Policies and Procedures on Business Associates.

CFBHN is not required to have such agreements with health care provider associates when disclosing information to them about patients they are treating.

Disclosure to Payers
§164.506(b)(3)

When making disclosures of PHI to an entity that is paying for treatment given by CFBHN, provide the minimum necessary PHI for the entity to make payment.

If a payer demands more information than you believe is necessary, or if the request is in some way non-routine (for example, when the payer is unknown or the payment has already been made), do the following: involve the Privacy Officer, have the payer fill out the *Payer Request for PHI* form, and follow the procedures above. Furthermore, make sure that the people requesting the information are who they claim to be and have the authority to receive the PHI. See the Verification Requirements section of these Policies and Procedures about

how to do that.

For payers seeking PHI for reasons related to operations, fraud and abuse detection, or compliance issues, ask them to confirm that they have or had a relationship with the patient. If they cannot confirm this, do not provide any PHI. Also ask them to confirm that they are classified as a "covered entity" under HIPAA. This simply means that they are required to comply with HIPAA just like CFBHN. If they are not a covered entity, you will have to decide what PHI to provide using the minimum necessary standard (see that section in these Policies and Procedures). If they are a "covered entity," ask them to describe the minimum necessary information they need to achieve their purposes. When they are a "covered entity," you can rely upon the payers' judgment about this, if it appears reasonable. You do not have to get a patient's authorization or consent, but are not prohibited from doing so.

For Marketing and Fundraising

CFBHN does not make these types of disclosures.

Workers Compensation
§164.512(l)

For disclosure for Workers' Compensation purposes, provide only the PHI necessary to comply with laws relating to Workers' Compensation, or other similar programs established by law, that provide benefits for work-related injuries or illness. You need not consider fault when making such disclosures nor get the patient's authorization or agreement to do so. Make sure that the people requesting the information are who they claim to be and have the authority to receive the PHI. See the Verification Requirements section of these Policies and Procedures about how to do that.

Public Health

Public Health Authority
§164.512(b)(1)(i)

Under HIPAA, CFBHN can, and may be required to by other laws, report PHI (such as vital records like births or deaths), to assist public health authorities in preventing or controlling disease, injury or disability. The Privacy Officer should preside over such disclosures, and file all associated documentation. The disclosed information should relate to activities such as public health surveillance, investigations and/or interventions. It should be given only to public health authorities authorized by law to collect this information and to foreign governments when CFBHN is directed to do so by such an authorized U.S. public health authority. CFBHN is not required to get authorization or agreement from patients when making such disclosures, but should disclose the minimum necessary PHI for this purpose.

Research
§164.512(i)

When research requests are made for CFBHN PHI, have the requestor fill out the Research

Request for PHI and get the relevant documentation. Also make sure that the people requesting the information are who they claim to be and have the authority to receive the PHI. See the Verification Requirements section of these Policies and Procedures about how to do that.

You may disclose PHI for research purposes, regardless of the funding source, if certain conditions exist or the researcher has met the proper criteria.

Alteration or Waiver of Authorization

If the researcher claims to have obtained an alteration or waiver, make sure that he or she provides documentation of the alteration/waiver with the request. That documentation must include the following:

- Identification of the Institutional Review Board (IRB) or a privacy board, and specification of the date of the action. If a privacy board is reviewing the documentation, the board must be comprised of members with various backgrounds and professional competency, have at least one member who is not affiliated with CFBHN, and have no board members with a conflict of interest. Review of research must occur at a meeting where the majority is present, including the member who has no affiliation. The majority present must agree. An expedited method can be used if it does not pose more than a minimal risk to the patients whose PHI will be used in the research.

- A statement that the IRB or privacy board has determined that the use of PHI will result in minimal risk to the privacy of the individuals based on an adequate plan of protection, a plan to destroy identifiers as soon as possible, and written assurances of protection.

- A description of the PHI requested.

- Statement that research could not be conducted without the waiver or alteration.

- Statement that research could not be conducted without access to the PHI.

- Review and Approval Procedures.

- Required Signature.

Reviews Preparatory To Research

CFBHN can disclose PHI to research organizations in preparation for conducting research if it first obtains from the researcher the following written assurances:

- The use or disclosure is to review PHI in order to prepare a research protocol or make other preparations for research.

- No PHI will be removed from CFBHN.
- The PHI being viewed is necessary for research purposes..

Research on Decedent's Information

CFBHN can disclose PHI on decedents to research organizations for research purposes if it first obtains from the researcher the following:

- Assurance that the use or disclosure being sought is solely for research on the PHI of decedents.
- Documentation of the death of such individuals.
- Documentation that the PHI being sought is necessary for the research purposes.

Research with Authorization

If the researcher will be providing the authorizations, make sure that the authorizations conform to the CFBHN requirements. Only provide PHI for each patient who has signed such an authorization.

If the researcher asks CFBHN to obtain the patient authorizations, have the researcher provide a list(s) specifying the patients for which he needs the PHI or provide a written description of the type of patient PHI he is seeking. CFBHN workforce members, who have access to the relevant PHI as a regular part of their job duties, will then ask patients to sign the authorizations.

Research with a Limited Data Set

If the researcher needs only limited data, establish a Data Use Agreement with the researcher. See the section in these Policies and Procedures on Limited Data Set and the requirements of a Data User Agreement.

People Who Might Have Been Exposed to Communicable Diseases
§164.512(b)(1)(iv)

CFBHN can, and may be required or allowed to by laws other than HIPAA, disclose relevant information to someone who might have been exposed to a communicable disease, or is at risk of contracting or spreading a disease or condition. The Privacy Officer should preside over such disclosures, and file all associated documentation. If there is any question about CFBHN's authority to communicate with the individual, ask the relevant public health authority (as described above) for permission regarding authority and contact with the individual. In either case, the information you provide should be relevant only to a health intervention or investigation. Furthermore, CFBHN is not required to get authorization or agreement from patients when making such disclosures.

People Responsible for Products Regulated by the FDA
§164.512(b)(1)(iii)

For products regulated by the Food and Drug Administration, CFBHN can report information to the persons (businesses) responsible for those products about the quality, safety and effectiveness of the products. The Privacy Officer should preside over such disclosures, and file all associated documentation. The disclosures can include information about harm caused by the product's misuse, defects, mislabeling and biological deviations. The purpose of these disclosures can include tracking/surveillance, enabling recalls, repairs, replacement or post-marketing surveillance. CFBHN is not required to get authorization or agreement from patients when making such disclosures, but should disclose the minimum necessary PHI for this purpose.

Employers
§164.512(b)(1)(v)

If reporting PHI to an employer is not a part of the routine at CFBHN, the Privacy Officer should preside over such disclosures, and file all associated documentation.

Make sure that the people receiving the information are who they claim to be and have the authority to receive the PHI. See the *Verification Requirements* section of these Policies and Procedures about how to do that.

For Disaster Relief
§164.510(b)(4)

You may disclose PHI necessary to a disaster relief agency to identify and locate a family member or personal representative of the patient, and to provide notification of the location, general condition or death of the patient. Such disclosures must be consistent with the wishes of the patient (see below about the presence and ability of the patient) and the need to respond to emergencies, but include the minimum necessary PHI. Make sure that the people requesting the information are who they claim to be and have the authority to receive the PHI. See the *Verification Requirements* section of these Policies and Procedures about how to do that.

Reporting on Crimes, Criminals, Victims and Inmates

Child Abuse
§164.512(b)(ii)

Under HIPAA, CFBHN can, and may be required to by other laws, report suspicions of child abuse. It can also provide PHI to public health authorities authorized by law to receive reports of child abuse or neglect. Use the form for *Disclosure of PHI for Abuse, Neglect and Domestic Violence and file all records*. The Privacy Officer should preside over such disclosures, and file all associated documentation. CFBHN is not required to get authorization or agreement from the patient or their representative when making such disclosures. Make sure that the people receiving the information are who they claim to be

and have the authority to receive the PHI. See the *Verification Requirements* section of these Policies and Procedures about how to do that.

CFBHN does not treat patients and does not relieve the subcontractor of their reporting requirements under the law and/or as required by regulations. CFBHN expects providers to make the reports as outlined by law and regulations.

Abuse, Neglect, and Domestic Violence Against an Adult
§164.512(c)

You can disclose the minimum necessary PHI of adults who are victims of abuse, neglect, or domestic violence, to a social service agency or law enforcement agency authorized to receive such information, under the following circumstances:

- A disclosure is required by law; or
- The individual agrees to the disclosure; or
- The disclosure is allowed by statute or regulation and, in your professional judgment, you believe a disclosure is necessary to prevent serious harm to the patient or other potential victims; or
- The disclosure is allowed by statute or regulation and, if the patient is unable to agree because of incapacity, a public official (including law enforcement) agrees that PHI will not to be used against the patient, and also claims that waiting for patient's consent would adversely affect related enforcement activities.

The Privacy Officer should preside over such disclosures, and file all associated documentation. Make sure that the people receiving the information are who they claim to be and have the authority to receive the PHI. See the *Verification Requirements* section of these Policies and Procedures about how to do that.

CFBHN is not required to get authorization or agreement from the patient or their representative when making such disclosures. However, when a disclosure is made under these circumstances, inform the patient as soon as possible that the disclosure has been made, unless you believe that informing the patient or representative could cause risk or serious harm.

CFBHN does not treat patients and does not relieve the subcontractor of their reporting requirements under the law and/or as required by regulations. CFBHN expects providers to make the reports as outlined by law and regulations.

Averting Threats
§164.512(j)(1)(i)

HIPAA allows, and other laws may require, CFBHN to disclose PHI necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. The

Privacy Officer should preside over such disclosures, and file all associated documentation. Such disclosures should be made to person(s) who are reasonably able to prevent or lessen the threat, which can include the person who is the target of the threat. CFBHN will have acted in good faith if the disclosure is based upon CFBHN's direct knowledge or CFBHN's reliance on a credible account by a person with apparent knowledge or authority. Authorization or the opportunity for the patient to agree or deny is not required. Disclose the minimum PHI necessary for this purpose. Furthermore, make sure that the people receiving the information are who they claim to be and have the authority to receive the PHI. See the *Verification Requirements* section of these Policies and Procedures about how to do that.

CFBHN does not treat patients and does not relieve the subcontractor of their reporting requirements under the law and/or as required by regulations. CFBHN expects providers to make the reports as outlined by law and regulations. Escaped Inmates
§164.512(j)(ii)(B)

HIPAA allows, and other laws may require, CFBHN to disclose PHI about a person who appears to be an escapee from a correctional institution or from lawful custody. The Privacy Officer should preside over such disclosures, and file all associated documentation. Authorization or the opportunity for the patient to agree or deny is not required. Disclose the minimum PHI necessary for this purpose. Furthermore, make sure that the people receiving the information are who they claim to be and have the authority to receive the PHI. See the *Verification Requirements* section of these Policies and Procedures about how to do that.

CFBHN does not treat patients and does not relieve the subcontractor of their reporting requirements under the law and/or as required by regulations. CFBHN expects providers to make the reports as outlined by law and regulations.

Reporting Violent Criminals
§164.512(j)(ii)(A)

CFBHN can disclose PHI to law enforcement authorities to help them identify or apprehend an individual who admitted to participating in a violent crime in which someone was seriously hurt. However, do not make such a disclosure if the statement occurred during treatment, counseling, or therapy (or request for such services) for the type of behavior that led to such a crime. The Privacy Officer should preside over such disclosures, and file all associated documentation. CFBHN can disclose only the following information concerning patients who make statements about participating in violent crimes:

- The statement (admitting participation in a violent crime);
- Name and address;
- Date and place of birth;
- Social Security number;
- ABO blood type and Rh factor;
- Type of injury;

- Date and time of treatment;
- Date and time of death (if applicable);
- Description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

Make sure that the people receiving the information are who they claim to be and have the authority to receive the PHI.

CFBHN does not treat patients and does not relieve the subcontractor of their reporting requirements under the law and/or as required by regulations. CFBHN expects providers to make the reports as outlined by law and regulations. Law Enforcement Disclosures
§164.512(f)(1)(i)

PHI may be disclosed to law enforcement officers as required by law. The Privacy Officer should preside over such disclosures, and file all associated documentation. If the disclosure results from a request, rather than CFBHN volunteering the information, ask whomever is requesting the information to cite the law. If you are unfamiliar with the stated law, check to make sure it indeed requires disclosure by CFBHN. You are not required to obtain patient authorization or to provide the patient with an opportunity to agree or object. Disclose the minimum necessary PHI for this purpose. Furthermore, make sure that the people receiving the information are who they claim to be and have the authority to receive the PHI

Legal Orders
§164.512(f)(1)(ii)

PHI may be disclosed in compliance with, and as limited by a court order, a court-ordered warrant, or a subpoena or summons issued by a judicial officer; a grand jury subpoena; an administrative request, including an administrative subpoena or summons; a civil or an authorized investigative demand; or similar process authorized under law. The Privacy Officer should preside over such disclosures, and file all associated documentation. Before making a disclosure, obtain a copy of whichever above-mentioned document applies. Furthermore, make sure that the people requesting the information are who they claim to be and have the authority to receive the PHI. See the *Verification Requirements* section of these Policies and Procedures about how to do that.

If the request for PHI is based upon an administrative request such as an administrative subpoena or summons, or a civil or investigative demand, the information sought must be:

- Relevant and material to a legitimate law enforcement inquiry; and
- Specific and limited to what is reasonably needed for the purpose for which the information is sought; and
- De-identified information could not reasonably be used.

You are not required to obtain patient authorization or to provide the patient with an opportunity to agree or object. Disclose the minimum necessary PHI for this purpose using the legal order as a guide. If the requestor seeks information that is inconsistent with what is

listed in the order, or appears inconsistent with a reasonable interpretation of what the order calls for (when the information is not listed), get legal assistance to determine the minimum necessary required by the order.

Identifying or Locating a Person
§164.512(f)(2)

PHI may be disclosed to a law enforcement official when he or she makes a request to help identify or locate a suspect, fugitive, material witness, or missing person. The Privacy Officer should preside over such disclosures, and file all associated documentationUnder the circumstances mentioned above, only the following PHI may be disclosed:

- Name and address;
- Date and place of birth;
- Social Security number;
- ABO blood type and Rh factor;
- Type of injury;
- Date and time of treatment;
- Date and time of death, if applicable;
- A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

Unless required by law, you may not disclose any PHI related to the individual's DNA or DNA analysis, dental records, typing samples, or analysis of body fluids or tissue.

You are not required to obtain patient authorization or to provide the patient with an opportunity to agree or object. Make sure that the people receiving the information are who they claim to be and have the authority to receive the PHI. See the *Verification Requirements* section of these Policies and Procedures about how to do that.

Victims of Crime
§164.512(f)(3)

PHI may be disclosed to a law enforcement official making a request for information about a patient who is, or is thought to be, a victim of a crime. The Privacy Officer should preside over such disclosures, and file all associated documentation. The patient must either provide consent, or be unable to provide consent because of incapacity or other emergency circumstances. For a patient who is able, use the *Disclosure* consent form even if he or she denies consent. If the patient is unable to provide or deny consent, you can disclose the PHI if:

PHI is needed to determine whether a violation of law has occurred, and such information is not meant to be used against the patient; and

- The law enforcement activity that depends on the PHI would be materially and adversely affected by waiting until the patient is able to agree to the disclosure; and
- In your professional judgment, you believe a disclosure is in the best interest of the patient.

Disclose the minimum necessary for this purpose. Make sure that the people requesting the information are who they claim to be and have the authority to receive the PHI. See the *Verification Requirements* section of these Policies and Procedures about how to do that.

Death due to Criminal Conduct
§164.512(f)(4)

If there is a reasonable suspicion that a patient died from criminal activity, you may alert law enforcement officials without obtaining the written authorization of the patient's representative, and without giving the patient/representative an opportunity to agree or object to the disclosure. The Privacy Officer should preside over such disclosures, and file all associated documentation. Furthermore, make sure that the people requesting the information are who they claim to be and have the authority to receive the PHI. See the *Verification Requirements* section of these Policies and Procedures about how to do that.

Crime on CFBHN Premises
§164.512(f)(5)

If a crime occurs on CFBHN premises the Privacy Officer should be involved in reporting the crime. It is recommended that the consent form be used if PHI is a part of what is reported. In the report to law enforcement officials, you can include PHI that is evidence of the crime without obtaining the written authorization of the patient or the patient's representative, and without providing the patient/representative an opportunity to agree or object to the disclosure. Include only the minimum necessary PHI that will provide evidence of the crime or help in catching the perpetrator.

Reporting a Crime in Emergencies
§164.512(f)(6)

CFBHN can, and may be required to by law (other than HIPAA), disclose to a law enforcement officials evidence of a crime discovered while providing emergency health care. The Privacy Officer should preside over such disclosures, and file all associated documentation. Furthermore, make sure that the people requesting the information are who they claim to be and have the authority to receive the PHI. See the *Verification Requirements* section of these Policies and Procedures about how to do that. It is not necessary to obtain written authorization or agreement from the patient or the patient's representative. However, make sure that any PHI included relates to the commission and nature of the crime; the location of the crime; the victims; or the identity, description and location of the perpetrator of the crime. If the crime is abuse, neglect, or domestic violence, see the section in these Policies and Procedures on *Abuse, Neglect, or Domestic Violence*.

Related to Inmates
§164.512(k)(5)

Although HIPAA privacy laws cover everyone receiving health care services from covered entities, there are certain requirements that do not apply when a person is incarcerated. These exemptions to specific requirements have been noted in these policies and procedures.

CFBHN may disclose PHI to a correctional institution or other law enforcement official who has lawful custody of an inmate or other individual, if the PHI is necessary for:

- Provision of health care to that person;
- Health and safety of that person or other inmates;
- Health and safety of the officers, employees, or others at the correctional institution, the persons responsible for transporting inmates, or other law enforcement officials;
- Administration and maintenance of the safety, security, and good order of the correctional institution.

This does not apply to persons who have been released on parole, probation, supervised release, or otherwise are no longer in lawful custody. The Privacy Officer should preside over such disclosures, and file all associated documentation. Patient authorization or opportunity for the patient to agree or object is not required. Disclose the minimum necessary PHI for this purpose. Make sure that the people requesting the information are who they claim to be and have the authority to receive the PHI. See the *Verification Requirements* section of these Policies and Procedures about how to do that.

Oversight of CFBHN, the Health Care System and Government Programs

Requests from the Secretary of the Department of Health and Human Services
§160.3 and §164.502(a)(2)(ii)

Disclosures to the Department of Health and Human Services are required for CFBHN; however, such disclosures do not require written authorization or agreement from the patient or the patient's representative. The Privacy Officer should preside over such disclosures, and file all associated documentation. Make sure that the people requesting the information are who they claim to be and have the authority to receive the PHI. See the Verification Requirements section of these Policies and Procedures about how to do that.

Other Requests for Use or Disclosure for Oversight Activities
§164.512(a) and §164.512(d)

CFBHN may disclose PHI to a health oversight agency for activities authorized by law and necessary for oversight of:

- The health care system; and

- A government benefit program for which health information is relevant to beneficiary eligibility. This includes non-health benefits programs if oversight of such a program

requires health information; and

- Entities subject to government regulatory programs for which health information is necessary for determining compliance; and

- Entities subject to civil rights laws for which health information is necessary for determining compliance.

Some examples of oversight activities include:

- Audits

- Inspections

- Licensure or disciplinary actions

- Civil investigations, proceedings or actions

- Administrative investigations, proceedings or actions

- Criminal investigations, proceedings or actions

Because their focus is oversight, these rules are not designed to permit other kinds of law enforcement investigations of an individual. Therefore, see the section Reporting on Crimes, Criminals, Victims and Inmates and form for *Disclosure of PHI for Law Enforcement* if the request is about an individual patient and the request it is not directly related to:

- The receipt of health care; or

- Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services; or

- A claim for public benefits if PHI is necessary to the investigation, which can include a benefits program that is not health-related.

The Privacy Officer should preside over such disclosures, and file all associated documentation. Make sure that the people requesting the information are who they claim to be and have the authority to receive the PHI. See the Verification Requirements section of these Policies and Procedures about how to do that. It is not necessary to obtain written authorization or agreement from the patient or the patient's representative for this type of disclosure.

Judicial or Legal Requests

Court Order or Administrative Tribunal Order
§164.512(e)(1)(i)

CFBHN does not treat patients and does not relieve the subcontractor of their reporting requirements under the law and/or as required by regulations. CFBHN expects providers to make the reports as outlined by law and regulations.

For an order from a court or administrative tribunal, you may disclose PHI only as it is expressly authorized in the order. Patient authorization or opportunity for the patient to agree or object is not required. The Privacy Officer should preside over such disclosures, and file all associated documentation.

Subpoena, Discovery Request, Other Lawful Process Without an Order
§164.512(e)(1)(ii)&(iii)

There are three circumstances where CFBHN can disclose PHI in response to a subpoena, discovery request, or other lawful process when the request is not accompanied by an order from a court or administrative tribunal.

First, you may disclose the requested PHI if you receive satisfactory assurance that the party seeking the PHI sincerely tried to provide a notice to the patient and the patient had an opportunity to object. This assurance should consist of documentation (such as the notice) and must include a signed statement from the requestor saying:

- The requestor made a good faith effort to provide a notice to the patient (which could have included sending it to the last known address of the patient); and
- The notice included enough information about the litigation or proceeding for the patient to object through the presiding court or tribunal. Even if a copy of the notice is provided in which the opportunity to object seems clear, the requestor must sign a statement saying that the patient had enough information to raise an objection; and
- The timeline provided for raising objections has expired and either no objections were filed, or the objections have been resolved through the court or tribunal to allow the disclosure.

Second, you may disclose the requested PHI if you receive satisfactory assurance that the party seeking the information made a reasonable effort to secure a qualified protective order. This assurance can consist of documentation (such as the protective order) and must include a signed statement from the requestor saying that:

- The parties involved have agreed to a qualified protective order and have presented it to the court or administrative tribunal; or
- The party seeking the PHI has requested a qualified protective order.

To be qualified, the order must be, or propose to be, an order of the court or tribunal, or a stipulation between the disputing parties. It must also prohibit the parties from using or disclosing PHI for any reason other than the litigation or proceedings for which the information was requested, and require that the PHI be returned or destroyed at the end of the litigation.

Third, CFBHN can agree to provide the above-described notice to the patient or seek the above-described qualified protective order. Note that the timeline for allowing the patient to object applies if a notice is issued.

If the above documentation is not provided and, therefore, you refuse to disclose the PHI to the requestor, you may have to seek legal counsel.

The Privacy Officer should preside over such disclosures, and file all associated documentation. Make sure that the people requesting the information are who they claim to be and have the authority to receive the PHI. See the Verification Requirements section of these Policies and Procedures about how to do that. Disclose the minimum necessary PHI for this purpose using the legal document (subpoena, summons, etc.) as a guide. If the requestor seeks information that is inconsistent with what is listed in the legal document, or appears inconsistent with a reasonable interpretation of what the legal document allows (when the information is not listed), get legal assistance to interpret the minimum necessary required by the document.

Military, National Security and Foreign Services

U. S. Military Personnel
§164.512(k)(1)(i)

Patient authorization or agreement is not required for disclosures of military personnel PHI if the appropriate military authority has published a proper notice in the Federal Register. To be proper, the notice must describe the appropriate military command authorities and describe the purpose for the use or disclosure of PHI.

The Privacy Officer should preside over such disclosures, and file all associated documentation. Ask the requestor to provide a copy of the notice. Also, make sure that the people requesting the information are who they claim to be and have the authority to receive the PHI. See the Verification Requirements section of these Policies and Procedures about how to do that. Disclose the minimum necessary PHI for this purpose using the notice as a guide.

Foreign Military Personnel
§164.512(k)(1)(iv)

Patient authorization or agreement is not required for disclosures of foreign military personnel PHI to the patient's military command, if the appropriate military authority has published a proper notice in the Federal Register. To be proper, the notice must describe the appropriate military command authorities and describe the purpose for the use or disclosure

of PHI.

The Privacy Officer should preside over such disclosures, and file all associated documentation. Ask the requestor to provide a copy of the notice. And make sure that the people requesting the information are who they claim to be and have the authority to receive the PHI. See the Verification Requirements section of these Policies and Procedures about how to do that. Disclose the minimum necessary PHI for this purpose using the notice as a guide.

Intelligence/Counterintelligence
§164.512(k)(2)

Patient authorization or agreement is not required for disclosures of PHI for U.S. national security and intelligence activities. CFBHN may disclose PHI to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, et seq.) and its implementing act (like Executive Order 12333).

The Privacy Officer should preside over such disclosures, and file all associated documentation. Ask the requestor to provide a copy of, or at least cite his authority, and provide documentation of their request. Furthermore, make sure that the people requesting the information are who they claim to be. See the Verification Requirements section of these Policies and Procedures about how to do that. Disclose the minimum necessary PHI for this purpose using the request as a guide.

Threats to Public Figures
§164.512(k)(3)

Patient authorization or agreement is not required for disclosures of PHI to officials providing protective services to the U.S. President or similar public figures (as authorized under 18 U.S.C. 3056 and 22 U.S.C. 2709(a)(3)) or performing related investigations (authorized under 18 U.S.C. 871 and 879).

The Privacy Officer should preside over such disclosures, and file all associated documentation. Ask the requestor to provide a copy of, or at least cite his authority, and provide documentation of the request. Furthermore, make sure that the people requesting the information are who they claim to be. See the Verification Requirements section of these Policies and Procedures about how to do that. Disclose the minimum necessary PHI for this purpose using the request as a guide.

Department of State Suitability Determinations
§164.512(k)(4)

If CFBHN is a component of the U. S. Department of State, patient authorization or agreement is not required for disclosures of PHI to officials making medical suitability determinations for the purpose of security clearances and availability to work abroad.

The Privacy Officer should preside over such disclosures, and file all associated documentation. Ask the requestor to provide a copy of, or at least cite his authority, and provide documentation of their request. Furthermore, make sure that the people requesting the information are who they claim to be. See the Verification Requirements section of these Policies and Procedures about how to do that. Disclose the minimum necessary PHI for this purpose using their request as a guide.

Financial Gain Other Than Billing for Services

Fundraising
§164.514(f)(1)

CFBHN does not conduct fund raising form patients served under the contracts and is prohibited from using or releasing PHI for any patients to any outside party.

Marketing
§164.508(a)(3)

CFBHN must obtain written authorization for any use or disclosure of PHI for marketing with these exceptions:

- A face-to-face communication made by CFBHN to an individual.
- A promotional gift of nominal value.

Otherwise, the patient or the patient's representative must complete an *Authorization to Use or Disclose PHI* form. If the marketing involves remuneration to CFBHN by a third party, CFBHN must say so in the *Authorization to Use or Disclose PHI* form.

Exceptions to Disclosure Restrictions for CFBHN Workforce members and Business Associates

Whistleblowers
§164.502(j)

Employees or Business Associates of CFBHN may disclose PHI without written authorization and without a formal request to the Privacy Officer when they believe, in good faith, that CFBHN:

- Engages or has engaged in unlawful conduct; or
- Violates professional or clinical standards; or
- Potentially endangers patients, workers or the public.

These whistleblowers may disclose PHI that is substantive to their concern, to:

- A relevant health oversight agency, public health authority or accreditation

organization; and/or

- An attorney retained by or on behalf of the whistleblower for the purpose of determining the whistleblower's legal options.

Workforce members Victims of Crime
§164.502(j)

A workforce member of CFBHN who is the victim of a crime may disclose the PHI of the suspected perpetrator to a law enforcement officer. The PHI disclosed must be limited to the suspect's:

- Name and address
- Date and place of birth
- Social Security number
- ABO blood type and Rh factor
- Type of injury
- Date and time of treatment
- Date and time of death, if applicable

Decedents

Generally, the same use and disclosure requirements apply to deceased patients as those that apply to living patients. However, there are some exceptions.

Medical Examiners
§164.512(g)(1)

CFBHN may disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law. The Privacy Officer should preside over such disclosures, and file all associated documentation. Make sure that the recipients are who they claim to be. See the Verification Requirements section of these Policies and Procedures about how to do that. Disclose the minimum necessary PHI for this purpose using their request as a guide.

Funeral Directors
§164.512(g)(2)

CFBHN may disclose PHI to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. The covered entity may disclose the PHI prior to the impending death of the patient. The Privacy Officer should preside over such disclosures, and file all associated documentation. Make sure that the recipients are

who they claim to be. See the Verification Requirements section of these Policies and Procedures about how to do that. Disclose the minimum necessary PHI for this purpose using their request as a guide.

Other Uses and Disclosures
§164.508

Uses and disclosures not specifically covered under any other standards in these Policies and Procedures require written authorization.

Authorization to Use or Disclose Protected Health Information

CFBHN does not treat patients and does not relieve the subcontractor of their reporting requirements under the law and/or as required by regulations. CFBHN expects providers to make the reports as outlined by law and regulations. In a case where a release of information is required then the follow will apply.

In all cases where use or disclosure requires patient authorization, the patient or designated representative must complete the *Authorization to Use or Disclose PHI* form. Assist the patient in completing this form, if necessary. The form must be written in plain language, and must contain:

- A description of the information to be used or shared; and
- The name or other specific identification of the person authorized to share or use the information; and
- The name or other specific identification to whom the covered health entity can disclose or share the information; and
- A description of the purpose of the requested use or disclosure of information; and
- An expiration date or an expiration event. The statement "end of research study," "none" or similar language is sufficient if the authorization is for use of disclosure of PHI for research. This may also include the creation and maintenance of a research database or research depository; and
- Signature of the person/representative and date and a description of the patient's or patient representative's authority; and
- Statement of the patient's right to revoke the authorization including the procedures to do this, and any exceptions.
- A reference to CFBHN's *Notice of Privacy Practices*.
- A statement that health plans can condition treatment, enrollment or eligibility on an authorization, if applicable. If CFBHN cannot do this, you must include a statement to that effect.

FREQUENTLY ASKED QUESTIONS

What is Protected Health Information?

Protected Health Information, or PHI, is information that meets four standards:

- PHI is information that is communicated or recorded in any medium, written records, oral communication and electronic media that must be protected. For example, if you are talking with a patient and discussing health conditions on the phone, you must be careful that someone in your lobby cannot hear this information. Additionally, information that is on a computer or sent via email must be protected. If you have a computer database of patient files, for example, you must be sure that access to this information is limited. You must also be careful when working on your computer, to protect information on your computer screen.

- PHI is information that is either collected by your organization or maintained by your organization. For example, you may have a patient's previous medical record that you did not originate; you must protect these records. Information that is forwarded to someone else must also be protected. For example, if your office forwards information to a billing agency to process your bills, this information must be protected. You are also responsible for ensuring that the billing agency is keeping information secure.

- PHI is information that identifies an individual or could identify an individual. This includes basic information such as the person's name, social security number, home address, phone number, and driver's license number. However, it also includes less obvious information like place of employment, names of relatives, or physical descriptions (gender or hair color). Federal law identifies this information as *individually identifiable information*.

- PHI is information that relates to the individual's condition, treatment, or payment in the past, present, or future. For example, discussions of a patient's previous condition that has long been cured must be protected. When you are discussing treatment with a patient, you must guarantee a secure setting.

How or when can PHI be used?

As previously stated, PHI can be used or disclosed for treatment, payment, or health care operations (see "What are treatment, payment or health care operations?"). There are two more *exceptions* when you may use and disclose PHI without patient/representative approval.

- Psychotherapy notes. If the person who wrote the notes is the same person who is treating the patient, psychotherapy notes can be used by: an organization for training programs; or for legal defense of the person who created the notes. Psychotherapy notes cannot be used for any other purposes.

- Marketing under special circumstances. To use PHI for marketing usually requires authorization from the individual. There are two exceptions when authorization is unnecessary: 1) if the communication with the patient is face to face; 2) when the

marketing is for a small promotional gift of nominal value provided by the organization. For example, patients sometimes receive free samples when they receive a prescription. This marketing device would not require the written authorization of the patient.

Who is included as an employee, Business Associate, or representative?

You include all employees who work with PHI in the course of meeting their job responsibilities: medical professionals who provide direct health care; or office support workforce members who record information, schedule appointments, and communicate with patients.

You include Business Associates or representatives used by CFBHN in delivering services. For example, a doctor's office using a billing agency or a laboratory for services would be included in this policy. When Business Associates are used, a written contract or agreement must be in place stating that the Business Associate will safeguard PHI, and follow the privacy policies established by CFBHN.

What does it mean to receive, create, use, or disclose PHI?

This simply refers to the use of medical information. For example, in the course of treating a single patient, a doctor's office may *receive* medical records from the patient's previous physician, or another physician also treating the patient. They may also *create* new records as they examine and treat the patient. They will *use* private information, such as medical conditions and medications, in order to treat the patient. They may also need to *disclose* the information, if patients request their records, or if patients are referred to another physician. The federal rules, and the policies of CFBHN, use the phrase "receive, create, use, or disclose" to cover all possible uses of PHI.

What is "treatment, payment or health care operations" (TPO)?

This simply refers to the ordinary operations of a hospital or doctor's office. Treatment is the actual medical treatment of an individual, and may include medical examinations, patient referrals, or patient conferences. Payment is the processing, billing, and collection of payment for services or medical supplies. Health care operations include business management and administrative activities required to provide services. For example, administrative procedures would include implementing security policies.

What are we required to do?

You are required to ask a patient before making any disclosures. You are required to track all requests for information and all disclosures that do not have a specific release of information or are not for payment. . You must document all of the following:

- The person and organization making the request;
- Date and time of the request;
- The specific PHI that is requested;
- The purpose of the PHI;

- Notification to the Patient;
- Patient authorization, restrictions or prohibition of the request.

If the patient grants disclosure, then you must document the following:

- Any restrictions on the PHI;
- The specific PHI being released;
- Date and time of the release;
- Location of the release (such as the delivery address).

All disclosure information should be reported to the Privacy Officer. An accounting of all disclosures must be maintained for six years.

When does the patient need to be notified?

The patient must be notified *before* the disclosure is made. The patient must have time to restrict the disclosure. It is the patient's right to agree to, prohibit or restrict the disclosure of PHI.

What does the patient need to know?

The patient needs to know everything about the disclosure *before* you disclose any PHI. Be sure to tell the patient *who* is requesting the information, *what* they are requesting, *why* they are making the request, and *when* they would like to receive it. It is the patient's right to agree to, prohibit, or restrict the disclosure of PHI.

Under what circumstances can PHI be used without patient authorization?

As you already know, PHI can be used for TPO. (For more information on TPO see "What is treatment, payment or health care operations?") *Any* use outside of the TPO standards, requires patient authorization.

However, there are special circumstances that would allow you to use PHI without patient authorization *or* allowing the patient an opportunity to agree or object. In most circumstances, these exceptions were created to protect the patient and public. You may use or disclose PHI without authorization or opportunity for the following reasons:

- Requirements of Law
- Public Health Activities
- Victims Of Abuse, Neglect, Or Domestic Violence
- Health Oversight Activities
- Judicial And Administrative Proceedings
- Law Enforcement Purposes
- Decedents
- Cadaveric Organ, Eye, Or Tissue Donation Purposes
- Research Purposes
- Aversions of Serious Threat To Health Or Safety

- Specialized Government Functions
- Workers' Compensation

When can PHI be disclosed without patient authorization and without allowing the patient to agree or object?

There are special circumstances allowing you to use PHI without patient authorization *and* without allowing the patient to agree or object. In most circumstances, these items were created to protect the patient and the public. You may use or disclose PHI without authorization or opportunity to object, for public health activities, victims of abuse, neglect or domestic violence, health oversight activities, judicial and administrative proceedings, decedents, cadaveric organ, eye, or tissue donation purposes, research purposes, aversions of serious threat to health or safety, specialized government functions, or for purposes of workers' compensation. The requirements for disclosure are summarized below.

Note: In every instance, you must include the Privacy Officer, and you must document all details of the disclosure. Even though the same notifications may not be required, you are always responsible for carefully documenting any disclosure.

For public health activities, when can PHI be disclosed without patient authorization and without allowing the patient to agree or object?

A public health authority may be authorized by law to collect PHI in order to prevent or control disease, injury, or disability. A public health authority includes anyone authorized by law to act in that capacity. Some examples of public health activities include: county health departments, a state welfare or child services organizations, or the Federal Drug Administration.

Public Health authorities are allowed to collect PHI for several reasons, and you are allowed to disclose such information without patient authorization and without allowing the patient to agree or object. For example, a public health department may collect vital records such as death and birth information or they may lead public health investigations into a widespread occurrence of a disease. Another example could include the Federal Drug Administration tracking a recalled medication, or investigating a drug or food supplement that may have negative side effects.

PHI may also be disclosed in cases of people being exposed to a communicable disease or at risk of contracting or spreading a disease. PHI may be disclosed in order to notify and/or treat an infected person.

PHI may also be disclosed to an employer if the employee is engaged in providing health care, as it relates to medical surveillance or to a work-related illness or injury. In this case however, the employer must provide notice to the employee that PHI will be disclosed.

For victims of abuse, neglect or domestic violence, when can PHI be disclosed without patient authorization and without allowing the patient to agree or object?

Patients who you suspect are victims of abuse, neglect, or domestic violence fall into a special category. Health care providers may disclose PHI to a law enforcement agency, if they

reasonably believe a patient may be a victim of abuse, neglect, or domestic violence.

In these cases, you must inform the patient that you plan to, or that you have, disclosed PHI. If, in your professional judgment, you believe that this may the patient them at further risk, the patient does not need to be notified. If you reasonably suspect that the personal representative may be the cause of the abuse or neglect, then you are not required to inform the representative either. These provisions of the law are meant to protect the patient and should be used only after careful thought.

For health oversight activities, when can PHI be disclosed without patient authorization and without allowing the patient to agree or object?

You may disclose PHI to a health oversight agency for their supervisory responsibilities. A health oversight agency is a government agency that has, as part or all of its responsibilities, oversight of any of the following:

- Healthcare organizations;
- Government benefit programs that use healthcare information to determine eligibility;
- Organizations that fall under government regulatory programs that use healthcare information;
- Organizations subject to civil rights laws for which health information is necessary in determining compliance.

A health oversight organization may collect PHI for audits, civil, administrative, or criminal investigations, inspections, licensure or disciplinary action, or other activities necessary for oversight. For example, a State department of business or commerce may need PHI in order to confirm that a medical professional is complying with state law.

There is *one exception* to this standard. If the individual is the subject of the investigation or activity, and it is not related to the receipt of health care or a claim for public benefits, then the PHI cannot be disclosed.

For judicial and administrative proceedings, when can PHI be disclosed without patient authorization and without allowing the patient to agree or object?

There are judicial and administrative proceedings that require PHI disclosure without patient authorization and without allowing a patient to agree or object. PHI can be disclosed under the following circumstances.

- You receive a court order.
- You receive a subpoena, discovery request, or other legal document AND a written statement of confidentiality.

The difference between a court order and other legal document is the source. A court order comes from a court and is signed by a judge and you must comply.

A legal document, like a subpoena, may come from an attorney in the course of trying or investigating a case. It is still a binding legal document, and in some cases is still signed by a

judge. However, you must meet the following additional requirements:

- You must get satisfactory assurance that the patient has been give notice from the party seeking the information. The party must provide a written statement that they have made a good faith attempt to contact the patient with sufficient notice and time. They must also demonstrate that the patient did not file objections or that the objections have been resolved.

OR

- The party seeking the information has secured a qualified protective order to keep the information secure. The qualified protective order must prohibit parties from using or disclosing the PHI for anything other than the current litigation and it must ensure that the PHI is returned to the originating organization or that it will be destroyed.

For law enforcement purposes, when can PHI be disclosed without patient authorization and without allowing the patient to agree or object?

You can disclose PHI to a law enforcement official or other government entity charged with this responsibility without patient authorization and without allowing the patient to agree or object for these reasons:

- You can provide PHI as already required by law. For example, suspected cases of child abuse or neglect must be reported to a law enforcement officer.

- Another example of PHI disclosures as required by law is court related requests. You can provide PHI in compliance with a court order, grand jury subpoena, or a civil administrative request. In this case, the PHI requested must be relevant to the situation; it must be specific and limited in scope, and should only be turned over when de-identified information could not be used.
- Limited information for identification and location purposes can be provided to law enforcement authorities without authorization or notice. You can provide PHI for identifying or locating a suspect, fugitive, material witness, or missing person. The following is the limited information that can be provided:
    - Name and address;
    - Date and place of birth;
    - Social security number;
    - ABO blood type and Rh factor;
    - Type of injury;
    - Date and time of treatment;
    - Date and time of death (if applicable);
    - A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars and tattoos.

You cannot disclose any PHI related to a person's DNA, dental records, or typing, samples or analysis of body fluids or tissue.

- If someone is a victim of a crime or suspected to be a victim of a crime, PHI can be disclosed. You must have the individual's consent to the disclosure, or proof that the individual is incapacity or emergency circumstances prevent obtaining consent.

- You may disclose PHI to a law enforcement officer about an individual who has died if there is suspicion that death may be the result of criminal conduct.

- You can also disclose PHI to a law enforcement official if you believe such information is evidence of criminal conduct that occurred on CFBHN's premises.
- Health care providers who are providing emergency health care, can disclose PHI to a law enforcement official in order to alert law enforcement to:
    - The commission and nature of a crime;
    - The location of such crime or of the victim(s) of the crime;
    - The identity, description, and location of the perpetrator of the crime.

For information about decedents, when can PHI be disclosed without patient authorization and without allowing the patient to agree or object?

You may disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased person, determining the cause of death, or other reasons. You may also disclose PHI to funeral directors, as necessary to carry out their duties with respect to the decedent. This does not require patient authorization.

For cadaveric organ, eye or tissue donation purposes, when can PHI be disclosed without patient authorization and without allowing the patient to agree or object?

You may disclose PHI to organizations engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation, and transplants. This does not require patient authorization.

For research purposes, when can PHI be disclosed without patient authorization and without allowing the patient to agree or object?

You may use and disclose PHI for research, regardless of the funding source, without patient authorization and without allowing the patient to agree or object. The following requirements must be met:

- A waiver authorization by An Institutional Review Board (IRB) or a privacy board must be in place. A privacy board must be composed of members with varying background and professions and must include at least one member who is not affiliated with the covered entity or with the research organization. The waiver must include identification of the board and date of action, protection of PHI and adequate written assurances, and a description of PHI requested. A review by the board must be signed.
- If the research organization reviews the PHI prior to research, you must be sure that released PHI is used only for preparing research protocol and that no PHI is removed

from the premises.
- Decedents' PHI can be used by research organizations that secure the contents.

In order to avert a serious threat to health or safety, when can PHI be disclosed without patient authorization and without allowing the patient to agree or object?

You can disclose PHI if:

- You believe, in good faith, that a disclosure of PHI is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public, and the disclosure is made to a person(s) reasonably able to prevent or lessen the threat. However, PHI related to counseling or therapy cannot be disclosed.
- It is necessary for law enforcement authorities to identify or apprehend an individual who has admitted to a violent crime and you believe serious physical harm may have occurred. You can also release PHI if it appears that a patient/ individual has escaped from a correctional facility or lawful custody.

For specialized government functions, when can PHI be disclosed without patient authorization and without allowing the patient to agree or object?

PHI can be disclosed for: military and veterans activities; national security and intelligence activities; protective services for the President and others; medical suitability determinations; correctional institutions and other law enforcement custodial situations; and government programs providing public benefits. Each circumstance has special requirements.

- You may disclose PHI of armed forces personnel for activities necessary by appropriate military command authorities.
- An organization that is a component of the Department of Defense or Department of Transportation may disclose to the Department of Veterans Affairs PHI of armed forces personnel upon their separation or discharge.
- An organization that is part of the Department of Veterans Affairs may use or disclose PHI for eligibility or entitlement for benefits.
- An organization may use or disclose PHI of foreign military personnel to appropriate foreign military authority for any of the reasons stated above.
- An organization may disclose PHI to federal officials for intelligence, counter-intelligence, and other national security activities under the National Security Act.
- An organization may disclose PHI to federal officials for the protection of the president, other heads of state, or foreign heads of state.
- An organization that is part of the Department of State may use PHI to make medical suitability determinations for security clearances, availability for service, or for families to accompany Foreign Service members abroad.
- You may disclose PHI to a correctional institution or a law enforcement official who has custody of an individual for: the provision of health care to that individual; for the health and safety of other inmates, officers or employees; and for law enforcement or administrative purposes. Once the individual has been released, paroled, or under supervised release, this standard does not apply.

- Government program organizations providing public benefits may use or disclose PHI for determining eligibility or enrollment. They may also disclose PHI to other government agencies if they both serve the same populations.

For workers' compensation purposes, when can PHI be disclosed without patient authorization and without allowing the patient to agree or object?

An organization may disclose PHI in order to comply with workers' compensation laws. In order to provide benefits for work-related injuries or illness without regard to fault, such information can be disclosed without patient authorization and without allowing the patient to agree or object.

AUTHORITY

45 CFR §164.502 (2002)
45 CFR §164.506 (2002)
45 CFR §164.508 (2002)
45 CFR §164.510 (2002)
45 CFR §164.512 (2002) and 45 CFR §164.514 (f) and (g) (2002)

2. Minimum Necessary Standard for Protected Health Information (PHI)

PURPOSE

This policy explains the process for ensuring the minimum necessary standard when disclosing protected PHI.

POLICY

1.1. CFBHN will recognize that the minimum necessary PHI should be used or disclosed whenever possible.
§164.502(b)
§164.514(d)

PROCEDURES

When using or disclosing PHI, or when requesting PHI from another covered entity, CFBHN must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. Minimum necessary standard applies in two major ways. First, it applies to procedures within CFBHN. Second, it applies to procedures for requesting or disclosing PHI.

Minimum Necessary Standard within CFBHN

CFBHN must restrict access to PHI based on the job functions of your workforce members, reflecting CFBHN's business practices and workforce. To do this, you must:

Identify PHI Users

In order to properly implement the minimum standard, you must identify those persons or classes of persons, as appropriate, in your workforce who need PHI to carry out their duties. In addition, you must identify the category or categories of PHI to which access is needed and any conditions appropriate to such access. For more information on how to do this, see the section in these policies and procedures on administrative actions – employee assignments.

Apply the Minimum Necessary Standard

After you have identified employees or groups of employees who need access to PHI, you must make reasonable efforts to limit their access to only the PHI that is necessary to carry out their duties.

Disclosing PHI

Determine Type of Request

If you receive a request for disclosure of PHI, you must first determine the type of request

according to Policy 1.0: Uses and Disclosures of Protected Health Information. Under the following circumstances, you do not have to meet the minimum necessary standards. You should disclose the information exactly as authorized or prepared.

- The information has been de-identified. See Policy 3: *De-Identification of PHI* §164.514(b).
- The information is a limited data set. See Policy 4: *Limited Data Set for PHI* §164.514(e).
- The information requires written authorization for disclosure. See Policy 1: *Uses and Disclosures of PHI* §164.508.

Apply the Minimum Necessary Standard

- **Routine Disclosures** – For any type of disclosure that it makes on a routine and recurring basis, CFBHN must limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure. Once these protocols are in place, the request does not need to be forwarded to the Privacy Officer. Instead, the request may be handled in accordance with the written procedures.
- **Non-Routine Disclosures -** For all other disclosures, the Privacy Officer must review requests for use or disclosure on an individual basis to be sure that the PHI requested is the information reasonably necessary to accomplish the purpose for which disclosure is sought. CFBHN should have established criteria to review non-routine disclosures. You may not use, disclose or request an entire medical record except when it is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request.

Reliance on Requests

CFBHN may rely on a requested disclosure as the minimum necessary for the stated purpose when:

- The disclosure is to an authorized public official.
- The PHI is requested by another covered entity.
- The PHI is requested by a member of the workforce or a Business Associate of CFBHN who will use the PHI for providing professional services to CFBHN.
- The PHI is requested for research purposes when all criteria for such disclosures have been met.

Making a Request for PHI and Applying the Minimum Necessary Standard

When you request PHI from other covered entities, CFBHN must limit each request to that which is reasonably necessary to accomplish the purpose for which the request is made.

Routine Requests for PHI

For a request that is made on a routine and recurring basis, you must use procedures that limit the PHI you have requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

Non-Routine Requests for PHI

For all other requests, CFBHN must develop criteria to limit the request for PHI to the information reasonably necessary to accomplish the purpose for which disclosure is sought. Review of requests for disclosures must be made on an individual basis in accordance with established criteria. You may not use, disclose or request an entire medical record except when it is specifically justified as reasonably necessary to accomplish the purpose of the use, disclosure or request.

Minimum Necessary Standard *Not* Required

The minimum necessary standard is not required for:

a. Disclosures to, or requests by, a health care provider for treatment.

b. Uses or disclosures made to the patient.

c. Uses or disclosures made with a valid authorization from the patient.

d. Disclosures made to the Secretary of the Department of Health and Human Services.

e. Uses or disclosures that are required by law.

f. Uses or disclosures required for compliance with the Privacy Rule.

FREQUENTLY ASKED QUESTIONS

What does the minimum necessary standard mean?

The minimum necessary standard is a federal rule that states that the use and disclosure of PHI should be limited to the minimum amount necessary to accomplish the stated purpose. For example, a doctor's office sign-in sheet should ask only for information that is absolutely necessary, such as the patient's name, date and time of arrival. It is unnecessary to ask for the patient's phone number or ailment. Remember, every patient who signs in is able to see the

information stored on such a sign-in sheet. Workforce members must not access information they do not need to accomplish their job. A receptionist usually does not need to study a patient medical record just to schedule appointments.

Note that this standard does not apply to treatment, payment or health care operations. A physician who is treating a patient, for example, has access to as much information as necessary. It also does not apply to communication with the patient.

This policy specifically states that special rules in other policies may apply the minimum necessary standard to treatment, payment or health care operations. If you are unsure if other policies apply, consult your policies and procedures manual or CFBHN's Privacy Officer.

What is the minimum necessary within CFBHN?

The minimum necessary standard applies to employees and information they can access. This policy requires that CFBHN identify persons and positions within the organization that need to access PHI in order to carry out their job responsibilities. For example, a doctor and office manager may need access to PHI, but the receptionist and accountant may not. Further, once you determine who has access, you must make sure that employees receive only information necessary to complete their jobs. For example, office managers need to access patient names, addresses, phone numbers and services rendered, but doctors need access to complete medical records. You should document the protected information held by CFBHN, the users of that information, and the need for each group of users to use or disclose the different parts of the information.

What is the minimum necessary standard for disclosures?

When CFBHN is disclosing information to a Business Associate, as a referral to another organization, or to the individual, minimum necessary standards apply. For any type of disclosure, disclosed PHI should be limited to the amount reasonably necessary to achieve the purpose for the disclosure. For example, if you are submitting information to a billing agency, only the information necessary to bill the patient or the insurance agency is disclosed. This may include disclosing the patient's name, address, insurance identification number, service rendered and fees. The patient's driver's license number, medical condition or weight would not be disclosed. If billing, referral or coordination of benefits is handled through industry standard claims forms, such as the UB-92 or the HCFA 1500, or is done electronically using standard transactions, you may complete all required elements on the form or transaction.

If a disclosure is made on a recurring basis, such as to the billing agency, then policies and procedures should be clearly defined and documented. The PHI disclosure must contain only information absolutely necessary. Disclosures *not* made on a regular basis must be considered and reviewed by the Privacy Officer.

Are there any exceptions to this minimum necessary standard?

Exceptions to the established minimum necessary standard are:

- Disclosures to a health care provider for treatment, payment or health care operations.
- Disclosures to the patient who is the subject of PHI.
- Disclosures to a public official with a valid authorization. A public official, such as a Department of Health employee with a valid authorization, should be provided with requested PHI.
- Disclosures requested by the Secretary of the Department of Health and Human Services.
- Disclosures required by law.
- Disclosures for compliance with the Health Insurance Portability and Accountability Act (HIPAA).
- Disclosures that require a written authorization from the patient. PHI should be provided in whole as stated in the written authorization.
- Requests for information by a professional who is a member of CFBHN's workforce or a Business Associate. The professional must assure that the information requested is the minimum necessary for the stated purpose(s).
- Requests for information for research purposes as long as all documentation is required in §164.512(i).

AUTHORITY

45 CFR §164.502(b) (2002)
45 CFR §164.514(d) (2002)

3. De-Identification of Protected Health Information (PHI)

PURPOSE

This policy explains the process of removing PHI identification elements to protect patient privacy.

POLICY

3.1. CFBHN will recognize that PHI can be de-identified and disclosed in certain circumstances.
§164.502(d)
§164.514(a) and (b)

3.2. CFBHN will recognize that de-identified information may be re-identified under specific circumstances.
§164.514(c)

PROCEDURES

De-Identification of PHI

De-identified information is information that does not identify an individual, or provide the possibility for an individual to be identified. CFBHN can use PHI to create de-identified data, or can disclose PHI to a Business Associate to create de-identified data. Once PHI has been de-identified, it is no longer PHI.

De-Identification of PHI

PHI can be de-identified in two separate ways. First, through the statistical method, and second, through the removal of identifiers.

Statistical Method. A person with appropriate knowledge and experience with statistical and scientific principles and methods may create an algorithm to de-identify the data if it is determined that the risk of identifying a patient by the information provided, or in combination with other information, is very small. Methods and results of analysis must be documented.

Remove Identifiers. To de-identify PHI, the personal identifiers must be removed and CFBHN must have no knowledge that the information could be used alone or in combination with other information to identify the patient. *All* of the following identifiers of the patient or of relatives, employers, or household members of the patient must be removed:

a. Names.

b. All geographic subdivisions smaller than a state. This includes 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,

- The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people.
- 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.

r. Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section.

Re-Identification of PHI

If you need to re-identify the de-identified information, you may assign a code or

other means of record identification to allow information de-identified to be re-identified, 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.

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

Disclosure of a code or other means of record identification used to re-identify data constitutes disclosure of PHI. Additionally, if such information is re-identified, the same requirements apply that apply to all other PHI.

FREQUENTLY ASKED QUESTIONS

What does "de-identified" mean?

Health information that does not identify an individual is considered "de-identified," which is usually achieved by removing names, Social Security Numbers, and all other patient-specific identifiers.

De-identified PHI is often used for research purposes. For example, a drug company may request de-identified PHI to help with efforts to improve asthma medications. You can provide PHI after it has been de-identified, without violating privacy rules.

How do you de-identify PHI?

You can de-identify PHI by removing information that might be used to identify the patient, relatives, employers, or household members. These elements are:

- Names.
- Geographic references smaller than a state, including street address, city, county precinct, and zip code (except for the first 3 digits).
- All dates except for year directly related to an individual, including birth date, admission date, discharge date, and date of death.
- Telephone numbers.
- Fax numbers.
- Electronic mail addresses.
- Social Security Numbers.
- Medical record numbers.
- Health plan beneficiary numbers.
- Account numbers.
- Certificate/license numbers.
- Vehicle identifiers and serial numbers, including license plate numbers.
- Device identifiers and serial numbers.

- Web Universal Resource Locators (URLs).
- Internet Protocol (IP) address numbers.
- Biometric identifiers, including finger and voice prints.
- Full face photographic images and any comparable images.
- Any unique identifying number, characteristic, or code.

What is "re-identification"?

You may assign a code or other means of record identification that will allow information that is de-identified to be used for contextual analysis. (Example: you may supply a file of de-identified patient demographics and a file of de-identified diagnosis information linked by a common identifier code. Your common identifier code, however, cannot be derived from any meaningful or related patient information and must not be disclosed. For example, before providing PHI to a researcher, you de-identify the information and assign random numbers to each PHI disclosure. You may keep a table or "key" to use in matching result records when they are returned by the researcher, but you must not disclose the "key" to the researcher.

Later, you can match the records to your master file of codes and identify the individual associated with each record. Remember, the codes must be kept confidential.

AUTHORITY

45 CFR §164.502(d) (2002)
45 CFR §164.514(a) and (b) (2002)
45 CFR §164.514(c) (2002)

4. Limited Data Set for Protected Health Information (PHI)

PURPOSE

This policy explains the process of creating Limited Data Sets for PHI to protect patient privacy.

POLICY

4.1. CFBHN will recognize that PHI can be provided in a limited data set in certain circumstances.
(§164.514(e))

PROCEDURES

Limited Data Sets

CFBHN may use PHI to create a limited data set, or disclose PHI to a Business Associate to create a limited data set. CFBHN may use or disclose a limited data set or disclose a limited data set when a current data set agreement is in place only for the purposes of research, public health or health care operations, when the need for the limited data set has been documented.

Limited Data Set
§164.514(e)

A limited data set is protected health information that excludes the following direct identifiers of the patient or of relatives, employers, or household members of the individual:

a. Names.

b. Postal address information, other than town or city, state, and full zip code.

c. Telephone numbers.

d. Fax numbers.

e. Electronic 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.

p. Full face photographic images and any comparable images.

Data Use Agreement
§164.514(e)

CFBHN may use or disclose a limited data set after obtaining satisfactory assurance, in the form of a data use agreement, that the limited data set recipient will only use or disclose the PHI for limited purposes. This may be modified, but at a minimum, it must:

a. Define the permitted uses and disclosures of the limited data set.

b. Establish who is permitted to use or receive the limited data set.

c. Provide that the limited data set recipient will:

- Not use or further disclose information other than as permitted by the *Data Use Agreement* or as otherwise required by law.
- Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the *Data Use Agreement*.
- Report to the covered entity any use or disclosure of the information not provided by its *Data Use Agreement*.
- Ensure that any agents, including subcontractors to whom CFBHN provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information.
- Not identify the information or contact the individuals.

Violation of the Data Use Agreement

If you know of a pattern of activity or practice by the recipient of the limited data set that constitutes a material breach or violation you must take reasonable steps to cure the breach or end the violation. If CFBHN is not able to do so, you must:

- Discontinue disclosure of the limited data set to the recipient.

- Report the problem to the Secretary of the Department of Health and Human Services.

A covered entity that violates a data use agreement is in noncompliance with the Privacy Rule, and must be reported to the Secretary.

FREQUENTLY ASKED QUESTIONS

What is a limited data set?

A limited data set has crucial identifying information removed from the data in order to protect a patient's privacy. In order to maintain this privacy, a limited data set ***cannot*** include any of the following:

- Names.
- Postal address information, other than town or city, state, and full zip code.
- Telephone numbers.
- Fax numbers.
- Electronic mail addresses.
- Social Security numbers.
- Medical record numbers
- Health plan beneficiary numbers.
- Account numbers.
- Certificate/license numbers.
- Vehicle identifiers and serial numbers, including license plate numbers.
- Device identifiers and serial numbers.
- Web Universal Resource Locators (URLs).
- Internet Protocol (IP) address numbers.
- Biometric identifiers, including finger and voice prints.
- Full face photographic images and any comparable images.

When is a limited data set used?

A limited data set is used for research, public health, or for health care operations. Research may include any collective work done by a university, institution, or public health department to gain a greater understanding of a health issue. For example:

- A medical school may use a limited data set to study the effects of a particular medication on people over 60 years old who have high blood pressure and diabetes.
- The Department of Health may use a limited data set to determine outbreaks of the West Nile Virus.
- Administrators may use data sets to develop procedures to implement new security

policies.

Who can receive limited data sets?

A limited data set can be shared with a contracted Business Associate, or anyone engaged in research, public health, or health care operations. A limited data set use agreement must be completed by anyone who makes a request, except for contracted Business Associates.

What is a Business Associate?

A Business Associate is any organization or individual with whom CFBHN works in the course of conducting business. This may include a laboratory that conducts tests for your patients, or a billing agency that bills patients and insurance companies. For purposes of this policy, Business Associates may see PHI. Use caution in making this determination.

Note: Business associates require contracts. For more information about the Business Associate Contract Form, see Policy 14: *Business Associates*.

What is a data use agreement?

A limited data set use agreement is a contractual document between CFBHN and the organization or individual who wants to use a limited data set for research, public health, or health care operations. The data use agreement is meant to provide a reasonable assurance that the organization obtaining the limited data set will not violate the use and disclosure terms of the agreement. The limited data set use agreement must establish the permitted and required uses and disclosures:

- Establish who is permitted to use or receive the limited data set.
- Requires that the recipient not use or further disclose the information other than as permitted by the agreement or required by law.
- Require appropriate safeguards to protect other uses and disclosures not allowed by agreement.
- Require reports to the covered entity of any inappropriate use or disclosure.
- Ensure that agents and subcontractors of the Business Associate also agree to the same restrictions and requirements.
- Not identify patient contact information.

What do I do if someone violates the data use agreement?

If there is a violation of the data use agreement by the Business Associate or other approved organization, you must do all of the following:

- Immediately report the problem to CFBHN's Privacy Officer.

- Terminate CFBHN's relationship with the organization immediately and discontinue the disclosure of the limited data set to the recipient.

- Report the problem to the Secretary of the Department of Health and Human Services.

AUTHORITY

45 CFR §164.514(e) (2002)

5. Verification Requirements for Use and Disclosure of PHI

PURPOSE

This policy explains the process of patient verification and authorization before use and disclosure of PHI.

POLICY

5.1. CFBHN will recognize the necessity to verify the identity of any individual or organization requesting PHI. (§164.514(h))

5.2. CFBHN will also recognize the necessity to verify the authority of any individual or organization requesting PHI. (§164.514(h))

5.3. CFBHN will also recognize that there are some circumstances under which the individual must be provided an opportunity to agree or object to PHI being used or disclosed. (§164.514(h))

PROCEDURES

Steps to Follow When Disclosing PHI

When disclosing PHI under any circumstances, it is the responsibility of CFBHN's Privacy Officer to verify the identification and authorization of the person requesting a disclosure of PHI, if the identity or authority is not already known to CFBHN.

Obtain Documentation

First, you must obtain any documentation, statements or representations, whether oral or written, from the person requesting the disclosure of PHI (§164.514(h)(1)(ii)). For example, a disclosure may be conditioned upon a subpoena or written authorization (§164.514(h)(2)(i)(A)).

Additionally, PHI disclosure may be restricted by a previous patient request. You must check the patient's records, and be sure you disclose only information that has not been restricted (§164.514(h)(1)(i)).

Verify the identities of individuals making the request

You must verify the identities of individuals requesting PHI.

a. **Patient, Representative or Health Care Provider** – If a patient, the patient's representative, or a doctor makes a request, you must confirm the requestor's identity, if the requestor is not already known to you (§164.514(h)(1)(i). If you

know the person, then confirmation is unnecessary. If you do not know the person, you should ask to see picture identification. Document that you verified the person's identity.

b. **Government Official** – If the disclosure is made to a public official, CFBHN may rely on any of the following to verify that individual's identity:

- An identification badge or other official credentials or proof of government status, if the request is made in person (§164.514(h)(2)(ii)(A)).
- Government letterhead, if the request is made in writing (§164.514(h)(2)(ii)(B)).
- A written statement on government letterhead, a contract or other type of signed agreement that indicates the person is acting under government authority, if the disclosure is to a person acting on behalf of a government official (§164.514(h)(2)(ii)(C)).

Verify the individual's authority to obtain PHI

a. If you are disclosing PHI to patients, they have a right to their information, and no verification of authority is necessary.

b. If a representative or family member of the patient is requesting PHI, you must verify his or her authority to receive such information (§164.514(h)(1)(i). This individual must be the legal guardian of the patient, or you must have a written statement from the patient that the individual can receive such information (§164.502). Check the patient's record to be certain there are no restrictions on disclosure to this individual.

c. If a doctor or other health care provider is requesting the PHI, you can disclose such information for purposes of treatment, payment or health care operations for the patient (§164.506).

d. If a public official is requesting the disclosure of PHI, you can rely on a written or oral statement of authority (§164.514(h)(2)(iii)(A)) or a legal process, warrant, subpoena, order or other legal process issued by a grand jury, judicial or administrative tribunal verifying the authority of the government official making the request (§164.514(h)(2)(iii)(B)).

In every case above, you should exercise professional judgment in determining whether or not a disclosure of PHI is justified (§164.514(h)(2)(iv)). Additionally, you should document all requests and actions, whether or not PHI is disclosed.

FREQUENTLY ASKED QUESTIONS

How do I verify the identity of a patient making a request?

Anytime you receive a request for PHI, you must verify the identity of the person making the request. Do not make the mistake of providing a person's PHI to a stranger who may be posing as the patient.

If the request is made in person, and you do not recognize the patient, you should ask to see picture identification. If you know the patient, then picture identification is unnecessary.

If the request is made over the phone, you should ask for some type of confirmation of identity. For example, you can ask the caller to recite the patient address, phone number, and full name.

In any case, you can rely on your professional judgment to confirm someone's identity. You must act on good faith in the best interests of the patient.

How do I verify the identity of another individual making a request?

If someone (health care provider, family member, or government official) is requesting PHI on behalf of a patient, you must confirm the identity and the authority of this person to see such information.

If it is a health care provider, you should take reasonable steps to confirm identity. For example, if you are mailing a patient's file to another physician, confirm the mailing address. If a courier picks up the information, be sure the file is properly sealed and request a confirmation of receipt.

If a patient representative is requesting such information, you should use picture identification to verify the representative's identity. If the request is made by phone, you should ask the caller to verify more information to confirm authorization to receive PHI on behalf of the patient. If possible, you should confirm this release with the patient. In all cases, document requests in the patient's file.

If the requestor is a public official, you can verify identity in person by viewing an agency identification badge or other documentation. You can verify identity of written requests by examining agency letterhead or other written documentation in which authority is issued, such as a contract or memorandum of understanding.

You must also verify the authority of the public official or written request. In some cases, however, this may not be necessary. For example, verification of authority is not necessary when the request is from the office of the Secretary of the Department of Health and Human Services.

When do I have to provide the individual with an opportunity to agree or object before PHI is used or disclosed?

You must provide an individual an opportunity to agree or object when you are using PHI in facility directories that include any of the following information: the individual's name, location

within your facility, descriptions of the individual's condition, or religious affiliation.

You must inform them of what is included in the directory and to whom you may disclose such information. They must be provided an opportunity to restrict or prohibit some or all of the information being used or disclosed.

In any case, you can rely on your professional judgment to confirm someone's identity. You must act on good faith in the best interests of the patient.

Note: Remember, only the Privacy Officer may disclose PHI.

AUTHORITY

45 CFR §164.514(h) (2002)
45 CFR §164.514(h) (2002)
45 CFR §164.514(h) (2002)

6. Patient's Right to Notice of Privacy Practices

PURPOSE

This policy explains the patient's right to receive a *Notice of Privacy Practices*.

POLICY

6.1. CFBHN will recognize the patient's right to receive a Notice of CFBHN's Privacy Practices.
§164.520(a) and (b)
§164.502(i)

6.2. CFBHN will recognize the patient's right to receive this notice no later than the date of the patient's first service delivery after April 14, 2003.
§164.520(c) and (d)

6.3. CFBHN will recognize its responsibility to post the notice in a clear and prominent location.
§164.520(c)

6.4. CFBHN will not require patients to waive their rights as a condition of treatment.
§164.530(h)

PROCEDURES

Privacy Restrictions

First, you must modify the HIPAA Click and Comply *Notice of Privacy Practices* form to include any CFBHN privacy restrictions that are more stringent than HIPAA requirements established in the prepared Notice.

The *Notice of Privacy Practices* must be written in plain language §164.520(b)(1). At a minimum, CFBHN must include in the *Notice of Privacy Practices* all of the following information:

- A header that reads: "THIS NOTICE DESCRIBES HOW YOUR MEDICAL INFORMATION MAY BE USED AND DISCLOSED AND HOW YOU CAN ACCESS THIS INFORMATION. PLEASE REVIEW THIS NOTICE CAREFULLY §164.520(b)(1)(i)."

- A description of the types of uses and disclosures that CFBHN can make, including an example (for patient comprehension) for treatment, payment, and health care operations disclosure §164.520(b)(1)(ii)(A).

  Note: All descriptions and examples that you provide must give the patient

enough detail to understand what PHI can be used or disclosed by CFBHN §164.520(b)(1)(ii)(D).

- A description of the types of uses and disclosures, including examples, that CFBHN can make that do not require patient authorization §164.520 (b)(1)(ii)(B).

  Note: If a use or disclosure is prohibited or limited by law, you must follow the more stringent law §164.520(b)(1)(ii)(C).

- A statement that all other uses and disclosures will require CFBHN to obtain the patient's written authorization and that the patient has the right to revoke an authorization §164.520(b)(1)(ii)(E).

  Note: If a use or disclosure is prohibited or limited by law, you must follow the more stringent law §164.520(b)(1)(ii)(C).

- A statement of the patient's rights regarding PHI and a description of how the individual may exercise these rights §164.520(b)(1)(iv) , including the right to request restrictions on certain uses and disclosures, the right to receive confidential communications, the right to inspect and copy PHI, the right to amend PHI, the right to a list of all disclosures, and the right to obtain a paper copy of this Notice. §164.520 (b)(1)(iv)(A) through (F)

- A statement that CFBHN is required to maintain the privacy of PHI, and that CFBHN is required to provide patients with notice of its legal duties and privacy practices with respect to PHI. §164.520(b)(1)(v)(A).

- A statement that CFBHN is required to abide by the current *Notice of Privacy Practices*. §164.520(b)(1)(v)(B).

- A statement that CFBHN reserves the right to change the terms of its Notice, to make the new notice provisions effective for all PHI, and a description of how patients will be notified of the changes §164.520(b)(1)(v)(C).

- A statement that individuals may complain to CFBHN, or to the Secretary of the Department of Health and Human Services, and that they will not be retaliated against for filing such complaints. The description must include a brief explanation of how to file a complaint §164.520(b)(1)(vi).

- An office employee contact name or title, and the telephone number so patients can obtain further information (§164.520(b)(1)(vii).

- An effective date for the *Notice of Privacy Practices*, which becomes effective after the notice is printed or published §164.520(b)(1)(viii).

There are some additional actions that require individual statements to be included in the Notice, if you intend to use them §164.520(b)(1)(iii). They are:

- If you contact a patient to provide appointment reminders, or information about treatment alternatives, or other health related benefits and services §164.520(b)(1)(iii)(A).

- If you contact a patient for fundraising purposes §164.520(b)(1)(iii)(B).

- If you are part of a group health plan, you may disclose PHI to the sponsor of the plan §164.520(b)(1)(iii)(C).

Note: You may choose to make the requirements for use and disclosure more stringent than HIPAA regulations. If you do, the requirements must be included in the *Notice of Privacy Practices*.

Posting Requirements

All CFBHN patients have a right to adequate notice of the uses and disclosure of PHI that may be made by CFBHN. They also have a right to know CFBHN's legal duties with respect to PHI. Therefore, this notice must be distributed and posted §164.520(a)(1).

There is one exception: An inmate does not have a right to *Notice of Privacy Practices* §164.520(a)(3).

Waiting Room Does not apply to CFBHN

Website

You must post a copy of the current notice on the CFBHN Website if CFBHN has one §164.520(c)(3)(i).

Public Request

You must give the notice to anyone who asks for it, regardless of whether or not the requestor is a Patient. You must also provide the notice to patients that may have already received the notice if they make another request. However, you are not required to give the notice to patients who are currently inmates in a prison or jail §164.520(a)(1) and (3) and (c)(2)(iii)).

Patients and Patient Representatives

Notice and Acknowledgement of Receipt

Patients/representatives who have not received the current version of the notice must be given the notice and an Acknowledgment of Receipt should be signed when they come to the office (see *Acknowledgement of Receipt* below). This should be done before treatment, including service delivered electronically. Once patients/representatives have received the Notice, they do not need to be given a copy thereafter, unless the notice has changed (this is discussed in "Changing the Notice") §164.520(c)(2)(i)(A) and (iii) (A).

Emergency Treatment

If emergency treatment prevents you from immediately giving patients the notice or obtaining the Receipt, follow procedure at the next available opportunity. Mail these documents if necessary (see Mailing the notice and *Acknowledgement of Receipt* below) 164.520(c)(2)(i)(B).

Remote Treatment

If the patients are treated remotely (by phone or email for example), mail the notice and Receipt to them on the same day they request service §(c)(3)(iii). See Mailing the notice or E-Mailing the notice and *Acknowledgement of Receipt* below.

Mailing the Notice

If you send the notice by regular mail, ask patients/representatives to promptly return the *Acknowledgement of Receipt* by mail or in person §164.520(c)(3)(ii). See *Acknowledgement of Receipt* below.

Emailing the Notice

If you send the notice by email, paste the notice text directly in the email message. DO NOT send it as an email attachment. Use the email feature that automatically sends a receipt back to you when the recipient opens the message. (For example, using Microsoft Outlook under the Options menu, check the box labeled, "Request read receipt for this message.") Since technical factors may prevent the automatic confirmation mentioned above, include a statement in the email similar to this: "Please reply to this message to show that you have received this notice of CFBHN's Privacy Practices." If you do not get email confirmation, mail the notice and Acknowledgement to the patient as previously described (§164.520(c)(3)(ii)). Upon request you must provide a paper copy of the notice to any individual who has received it electronically (§164.520(c)(3)(iv)).

Acknowledgement of Receipt

Ask patients/representatives to sign, date and return the *Acknowledgement of Receipt* for CFBHN's *Notice of Privacy Practices*.

Place a copy of the *Acknowledgement of Receipt* in patients' files. If you do not get a Receipt, document in the patients' files that you gave them the notice but you were unable to obtain a receipt. Your documentation must include an explanation of the reason why it was not obtained. CFBHN can still treat the patient as long as CFBHN made a good faith effort to get the Receipt. Good faith means that you will try the process again if you have reason to believe that the patient/representative did not actually get the notice (for example, you know that the emailed notice did not arrive), or the patient did not understand the need to return the receipt, you will try another way to get the notice to them. §164.520(c)(2)(ii).

Changing CFBHN's Notice of Privacy Practices

Any changes to the notice must be consistent with Federal, State, and professional rules, regulations and laws. Before implementing any new practices that are different from the practices described in the existing Notice, you must do the following §164.520(c)(2)(iv):

Change the Notice to reflect the new practices.

As a part of change, indicate the date the new practices will be put into effect on the notice and *Acknowledgement of Receipt* (both should show the same date). Implementation date must be after you have completed the process of change.

Change the version number

You must change the version number (next to the date) on the Notices and Acknowledgements of Receipt by one to indicate different versions. For example, the first notice posted by CFBHN will show a number 1; the second, a number 2, will allow you to keep track of how many versions of the notice have been posted and which version the patient acknowledged.

Replace the old Notice

You must replace the old notice posted in the waiting area(s) with the new Notice. You must replace the old notice posted on the Web site with the new Notice. You must begin distributing the new notice to patients/representatives when they visit the office and/or are treated by CFBHN.

Notify Patients

HIPAA does not require CFBHN, as a health care provider, to mail the new version of the notice to all of the patients on file, however, you must make it available upon request. Check to make sure no other laws require you to do so.

The notice should include the following statements:

"*Before making changes to the CFBHN Practices, a new Notice will be distributed to patients when they are treated by CFBHN.*

"*These n*ew *practices will apply to all information held by CFBHN*."

If the above statements appear in all versions of the Notice, HIPAA does not require CFBHN to handle patient records differently despite the fact that not all patients/representatives have seen the same Notice. Check to make sure no other laws require you to do so.

Copy Retention

You must retain copies of all versions of the Notice, and written acknowledgements of receipt or documentation of your good faith efforts to obtain a written acknowledgement §164.520(e) for at least six years §164.530(j).

FREQUENTLY ASKED QUESTIONS

Who has to have a Notice of Privacy Practices?

All covered entities that maintain PHI, or that use or disclose PHI, must have a *Notice of Privacy Practices*. CFBHN must have a *Notice of Privacy Practices*. There is one *exception*: correctional institutions do not have to provide a *Notice of Privacy Practices*.

What is a Notice of Privacy Practices?

A *Notice of Privacy Practices* is a document used to inform patients and patient representatives of their rights to related to the use and disclosure of their PHI. CFBHN must create a *Notice of Privacy Practices* that provides the procedures for handling PHI. CFBHN must also ensure that every patient it serves receives this Notice. A notice is provided with these documents.

Every patient has a right to this Notice, with one *exception*: an inmate does not have a right to notice, and the requirements do not apply to a correctional institution.

What does the Notice of Privacy Practices state?

The *Notice of Privacy Practices* must be written in plain language and must include:

- A header that reads: "THIS NOTICE DESCRIBES HOW YOUR MEDICAL INFORMATION MAY BE USED AND DISCLOSED AND HOW YOU CAN ACCESS THIS INFORMATION. PLEASE REVIEW THIS NOTICE CAREFULLY."

- A description of the types of uses and disclosures that CFBHN can make, including an example (for patient comprehension) for treatment, payment, or health care operations disclosure.

- A description of the types of uses and disclosures that CFBHN can make that require CFBHN to obtain the patient's written authorization.

- A statement that any other uses or disclosures (except treatment, payment or health care operations) will be made only with the patient's written authorization and that the patient has the right to revoke an authorization.

- A statement of the patient's rights regarding PHI and a description of how the individual may exercise these rights, including the right to request restrictions on certain uses and disclosures, the right to receive confidential communications, the right to inspect and copy PHI, the right to amend PHI, the right to a list of all disclosures, and the right to obtain a paper copy of this Notice.

- A statement that CFBHN is required to maintain the privacy of PHI, and that CFBHN is required to provide patients with its *Notice of Privacy Practices*.

- A statement that CFBHN is required to abide by the current *Notice of Privacy Practices*.

- A statement that CFBHN reserves the right to change the terms of its notice and to make the new notice provisions effective for all PHI.

- A statement with instructions on how an individual may complain to CFBHN, or to the Secretary of the Department of Health and Human Services.

- An office employee contact name or title, and the telephone number so patients can obtain further information.

- An effective date for the *Notice of Privacy Practices*, which becomes effective after the notice is printed or published.

There are some additional actions that require additional statements to be included in the Notice. Such statements are necessary:

- If you contact a patient to provide appointment reminders, or information about treatment alternatives, or other health related benefits and services.

- If you contact a patient for fundraising purposes.

- If you are a group health plan, you may disclose PHI to the sponsor of the plan.

Note: You may choose to make the requirements for use and disclosure more stringent than HIPAA regulations.

How do you post and distribute the Notice of Privacy Practices?

You must keep the CFBHN *Notice of Privacy Practices* posted in the office. It must be in a clear and prominent location where your patients can see and read the Notice.

You must provide the notice at the time of a patient's first service, effective April 14, 2003. In an emergency treatment situation, the notice is provided following emergency service and as soon as possible.

You must make a good faith effort to obtain written acknowledgement that patients have received the *Notice of Privacy Practices*. If you cannot obtain a written acknowledgement, you must provide a written explanation of why it was not obtained and post it in the patient's file.

If CFBHN maintains a website, then the *Notice of Privacy Practices* must be posted on the website. Additionally, if a patient has agreed to email notification, you may send the notice via email. An *Acknowledgement of Receipt* may also be sent via email. However, individuals who receive Notices by email also have the right to request hard copy of the Notice.

CFBHN must keep all documentation associated with the Notice, including the written Notice, the locations where it is posted, a record of who received the Notice, and all acknowledgements

of receipt.

Note: Remember, if no acknowledgment of receipt exists, you must provide an explanation.

How do you change or update the Notice of Privacy Practices?

CFBHN must revise its *Notice of Privacy Practices* whenever there is a material change to: the uses or disclosures; the patient's rights; or CFBHN's legal duties or other privacy practices. These changes cannot be implemented without a change to the *Notice of Privacy Practices*.

Note: Any time a change is made, you must retain and file all Notices of Privacy Practices.

AUTHORITY

45 CFR §164.520 (a) and (b) (2002)
45 CFR §164.520 (c) and (d) (2002)
45 CFR §164.520 (c) (2002)
45 CFR §164.520 (e) (2002)
45 CFR §164.530 (h) (2002)

7. Patient's Right to Access Protected Health Information (PHI)

PURPOSE

This policy explains the process for providing Patient Access to PHI.

POLICY

7.1. CFBHN will recognize the patient's right to access PHI.
§164.524

7.2. CFBHN will respond to requests for access to PHI within thirty (30) days. If CFBHN requires more time to process a patient request, the patient must receive notice.
§164.524(b)

7.3. CFBHN will accommodate the patient's right to complain and appeal this process.
§164.524(d)

7.4. CFBHN will maintain accurate records and reports to demonstrate compliance with this policy.
§160.310

PROCEDURES

Patients have a right of access to inspect and obtain a copy of PHI for as long as the PHI is maintained, with some exceptions.

Patient/Representative Request for PHI

Provide a Request for Protected Health Information form

Have patients/representatives fill out the *Patient Request for Access to Protected Health Information* form used by CFBHN. Assist patients/representatives in filling out the form, if necessary (§164.524(a)(1)). Do not ask Patients/Representatives the reasons for making the PHI request.

Proper Identification

Make sure that persons making a request are who they claim to be. For an individual making a request on behalf of a patient, verify his or her relationship with the patient. Make sure that when (if) you provide access to the PHI, it is to the right file as well as the right person. For example, if the request is for John Smith's records, make sure the file you access pertains to the John Smith you have just identified.

Sign and Date Request

Try to get patient/representatives to sign and date requests, regardless of who wrote them. If the patient/representative refuses to sign and date a request, note and initial that on the

original request.

Provide to Privacy Officer

Immediately give the request to the Privacy Officer.

The Privacy Officer will:

Discuss the PHI request with patient/representative

Discuss the scope of the request with the patient/representative. Complete the *Response to Request for Access to PHI* form.

a. **Request for Portion Only**
If patients/representatives care to see only a portion of the record, this will save effort for CFBHN and allow for faster responses.

b. **Summary or Explanation**
If Patients/Representatives want a written summary or explanation of a file, make sure that Patients/Representatives understand CFBHN's fees for preparing such documents before committing to the request (§164.524(c)(2)(i)).

Confirm Availability of Information

Check to make sure that CFBHN actually possesses the information being requested. If not, use the CFBHN Response to Patient Request for Access to Protected Health Care Information Form to inform Patients/Representatives that CFBHN does not have the information. Suggest where it can be found, if you know or can easily find out §164.524(d)(3).

Check to Make Sure there are no Reasons to Deny Access

Check to make sure there are no reasons to prevent Patients/Representatives from seeing part or all of the record. Determine what portion (if any) of the record can be provided, and follow procedure. This may mean providing only parts of the record or making parts of it unreadable (§164.524(d)(1)), as documented below.

Reasons to Deny Access

Confidential Communications

If a patient has asked for confidential communications with CFBHN, do not provide access to a Representative of a Patient unless you have gotten prior, confidential approval from the Patient. Show the Representative only the portion of the file that the Patient is willing to disclose (§164.522(a)).

Protecting Confidential Sources of Information

Determine if the record contains any information obtained by CFBHN from confidential sources other than a health care provider. Keep this information and the source of the information confidential (§164.524(a)(2)(v)).

Risks of Harm

Determine if harm could come to the Patient or others, if access is granted. This information should be discussed with health care professional(s) most involved in treating the Patient. Consider these examples:

- Suspected Abuse: If a Representative is granted access to a record (part or whole) where abuse of the Patient is suspected, and the Representative could be involved in the abuse, do not share the suspected information with the Representative until the suspicions are resolved (§164.524(a)(3)(iii)).

- Emotionally Unstable: If the Patient is emotionally unstable (in the judgment of the health care professional) and the information (part or whole) may cause the Patient to harm him/herself or others, do not share that information without taking steps to prevent such harm (§164.524(a)(3)(i)).

- Other Person: If some of the information in the Patient's file is about someone other than the Patient, and revealing it could cause harm to the other person (excluding health care providers when the "information" pertains to the professional responsibilities to a patient), do not share that information (§164.524(a)(3)(ii)).

Legal Matters

Do not share any material, which you think may be used, or is being used, in legal matters, audits and/or investigations (§164.524(a)(1)(ii)). This includes civil, criminal, and administrative actions or proceedings. However, the underlying information should be shared. For example, documents being prepared specifically for a lawsuit regarding the way that CFBHN has treated a patient should not be shared, but the Patient's diagnosis and treatment can be disclosed.

Audits or Investigations

Do not share any material gathered for a government/regulatory administrative action, such as an audit or investigation. However, the underlying information can be shared (see above).

Criminal Investigations

Check to make sure that no criminal investigators have requested any valid restrictions on sharing the information. However, the underlying information can be shared (see above).

Psychotherapy Notes

Do not share any psychotherapy notes (§164.524(a)(1)(i)).

Research Studies

Determine if the information is a part of an ongoing licensed study and providing

information may disrupt the Patient's participation in the study. If so, discuss the situation with the CFBHN medical professional most involved with the Patient. A judgment should be made in the best interest of the Patient. This may result in giving the Patient the information, thus dropping him/her from the study (§164.524 (a) (1) (iii) and (2) (iii)).

Inmate Requests

Patients who are currently inmates in a prison or jail may read, but may not receive, copies of their PHI without the approval of a prison/jail official and barring any other restrictions mentioned in the policy (§164.524 (a) (2) (ii)). Additionally, if you are a health care provider under the direction of a correctional institution, you may deny access to copies of PHI.

Clinical Laboratories

Organizations subject to the Clinical Laboratory Improvement Amendments (§493.3(a)(2)), may not be required to disclose PHI. In most cases, a doctor's office does not meet this standard; however, if you think CFBHN may, you should consult this rule.

CFBHN does not maintain requested PHI

If CFBHN does not maintain the requested PHI, you cannot provide access to that PHI. However, if you know where the requested information is maintained, you must inform the patients where to direct their requests for access.

If there is No Reason to Deny Access to PHI

If there is no reason to deny access to all or part of the record:

Arrange for Patient/Representative Access to the Requested PHI

Arrange a mutually convenient opportunity for the patient/representative to see the record and/or get copies of it (§164.524(b)(2)(i)(A) and (c)(i)).

Respond to Patient Request for Access to PHI Form

Complete and provide the Patient/Representative with a CFBHN *Response to Patient Request for Access to Protected Health Care Information* form and place a signed copy on file. See previous procedures for a patient unwilling to sign the form.

Provide Copies of PHI

If you are providing copies, do so in the format most preferred by the Patient/Representative, if it is easy for CFBHN to do so. For example, provide an electronic copy if the records are electronic and the patient prefers getting them that way (§164.524(c)(2)(i)).

Do not provide two copies of the same information simply because it appears in

two different places among CFBHN's records (§164.524(c)(1)).

Summary or Explanation of Record

You may provide a summary or explanation of the record, if the Patient agrees to accept and pay any charges for preparing it ahead of time (§164.524(c)(2)(i)).

Preparation Expenses

You may charge the Patient/Representative only the cost of providing the information:

- For paper copies, charge CFBHN's per paper copy rate (§164.524(c)(4)(i)).
- For information on a floppy diskette which you provided (warning, do not use a diskette provided by the Patient/Representative unless you are sure it does not contain a computer virus) (§164.524(c)(4)(i)).
- For applicable postage fees (§164.524(c)(4)(ii)).
- For an agreed upon fee for preparing any summary or explanation of the record. That charge must not exceed the cost of preparing this information (§164.524(c)(4)(iii)).

Denying Access to PHI

If there is a reason to deny access to part or all of the requested PHI, follow these procedures:

Provide a Response to Patient for Denial of Access Form

Provide whatever portion of the record you can as described above.

Complete and provide to the Patient/Representative a CFBHN *Response to Patient for Denial of Access Form* and place a copy on file (§164.524 (d) (2)). The statement must include:

- The basis for the denial;
- A statement of the patient's right to a review of denial;
- A description of how the patient may complain to CFBHN or to the Secretary of the Department of Health and Human Services.

Be careful when explaining the reasons for the denial to make sure that the explanation itself does not reveal information that should be kept confidential. For example, your explanation should not compromise an ongoing criminal investigation, suspicions of abuse, the confidentiality of the patient, or confidential sources.

Provide for a Review of Denial

If the patient/representative disputes the denial, give a copy of the Request Form, the Response Form, and any written dispute from the Patient/Representative, to a CFBHN licensed health care professional not involved in making the decision to deny access, who is the designated reviewing official. This professional will review and make the final decision for CFBHN (§164.524(a)(4) and (d)(4)).

Review of Decision to Deny Access

If the reason for denying access is to prevent harm to the Patient or others, then the health care professional should review the decision. The health care professional does not have to review when:

- The information was a part of a study. However, if the best interest of the Patient may be affected by not providing the information, the health care professional should review the decision.
- The information is expected to be a part of a civil, criminal or administrative proceeding.
- The information is psychotherapy notes.
- The information was withheld to protect the confidentially of the Patient or the confidentiality of someone who provided the information to CFBHN in confidence.
- Copies of PHI were withheld from an inmate in a correctional facility, or by a health care provider acting under the direction of a correctional institution.

If the health care professional changes the original decision, fill out a new CFBHN *Response to Patient Request for Access to Protected Health Care Information* form, give it to the patient for his/her signature, and place a signed copy in the file. If the Patient refuses to sign, follow previous procedures.

Meet Timelines

30-Day Response

You must complete the above procedures within 30 days from the date of the request from the Patient/Representative (§164.524(b)(2)(i)).

Additional 30-Day Extension

Fill out the CFBHN *Response to Patient Request for Access to Protected Health Care Information* form before the 30-day deadline to inform the Patient/Representative that CFBHN will require more time. Include the reason for the delay and when access will be provided (§164.524(b)(2)(iii)). Note: Only

one extension is allowed (§164.524(b)(2)(iii) (B)).

Patient Records Off-Site

If the reason for the delay is because the requested Patient records are not held on-site by CFBHN, 60 days (beyond the original 30) is allowed (for a total of 90) (§164.524(b)(2)(ii)).

Other Delay

Otherwise, only 30 more days are allowed (for a total of 60 days from the date of request) (§164.524(b)(2)(iii)).

Record Retention

CFBHN must retain the designated set of record that are subject to access by patients.

CFBHN must also keep the title of the persons or offices responsible for receiving and processing requests for access by patients.

FREQUENTLY ASKED QUESTIONS

How do patients request to see PHI?

Patients have the right to access their PHI. CFBHN provides a form to patients who request access. CFBHN will help patients complete the form; this may include filling out the form for the patient. Patients do not have to provide a purpose for seeing PHI, and are entitled to as much of the information as they would like, with some exceptions. This may include an entire medical history or one diagnosis.

I received a request from a patient for PHI… now what?

After you receive a request from a patient, you have 30 days to respond. If you cannot respond within 30 days, you must provide the patient with a written statement for the delay and the date by which you will fully respond to the request. You are allowed only one extension of time per request for PHI.

If the request is for PHI that you do not maintain onsite or is not accessible onsite, then you have 60 days to take action on the request, and you must notify the patient.

When you receive a request for PHI, you must verify the identity of the person making the request. If the patient/representative makes the request in person, then picture identification may be used. If the request is written, then the patient's signature and personal information can serve as confirmation. If a request is made over the phone, ask the patient/representative to confirm personal information you have on file. In any case, identity must be confirmed and should be documented and placed in the patient's file.

Does a patient have access to the entire PHI?

Even though patients have the right to see PHI, laws may prevent access to certain parts of the

information. They have a right to access all PHI, **except:**

- **Psychotherapy notes**. To protect and better serve the patient, professional notes, made in the course of a psychotherapy session, cannot be accessed by the patient/representative.

- **Information collected for use in a civil, criminal or administrative action, or proceeding**. This information, if it is for use in a legal or administrative case being prepared, may be denied to the patient/representative. However, the underlying PHI should be provided to the patient/representative.

- **PHI maintained by an organization covered under the Clinical Laboratory Improvements Amendments of 1988 (42 USC 263a).** PHI that is specifically exempt from these Amendments (§493.3(a)(2)) is denied access. For example, lab test results are sent to the hospital or doctor who requested them.

- **PHI requests made from a correctional facility or organization representing a correctional facility**. An inmate's request for copies of PHI may be denied if the access jeopardizes the health, safety, security, custody, or rehabilitation of the inmate or other inmates. Also, copies of PHI may be denied if the disclosure jeopardizes the safety of any officer, employee, or other person at the prison or interferes with treating or transporting the inmate.

- **Information obtained during the course of research**. If a patient is part of an ongoing research study, then access to PHI may be temporarily suspended as long as the study is in progress. However, the patient must have agreed to a denial of access when contracted to participate in the research project. Once the study is concluded, access to PHI may be resumed.

- **Records subject to the Privacy Act (5 USC 552a).** If the PHI is in a record that is subject to the Privacy Act, then access may be denied. (For examples, consult the Federal Register.)

- **Information obtained from someone other than a health care provider under a promise of confidentiality**. If PHI is obtained from someone who has been promised confidentiality, then access may be denied to the patient/representative. In other words, if you receive information granted by a confidential source, you are bound to that confidentiality and cannot disclose it.

- **Professional Judgment:** Access may be denied if a licensed health care professional determines, in the exercise of professional judgment, that access to PHI may endanger the life or physical being of the patient or another person.

- **The PHI makes reference to another person who is not a health care**

provider. A licensed health care professional, in the exercise of professional judgment, may deny access if the PHI could cause substantial harm to the person.

- **The request for PHI is made by the patient's personal representative**. A licensed health care professional, in the exercise of professional judgment, may deny access if the PHI could cause substantial harm to the patient or another person. For example, if a patient asks for confidential communications with CFBHN, the information should not be shared with a patient representative.

How do I provide access to PHI?

Once you review the request and the patient's request is accepted, you must provide the PHI. CFBHN and the patient must decide on an agreeable format for releasing the PHI.

You must provide the exact information requested. If you maintain duplicates, or the requested information appears in more than one location, you are required to provide access to only one. It is not necessary to prepare duplicate files for inspection.

In some cases, you may be asked to provide the patient/representative with a summary or explanation of the PHI. You must notify the patient in advance if CFBHN will charge a fee for this type of preparation.

Once patients are notified that they can access the requested PHI, the information must be provided in a timely manner, which includes arranging a time and place to inspect the PHI, or receiving a copy. If the patient/representative agrees, the information may also be mailed.

If you are preparing materials for the patient, you may charge fees for:

- Copies
- Postage
- A written summary or explanation

Remember to document any use or disclosure. For more information see "What are we required to do?" under Disclosures – Individual Rights.

How do I deny access to PHI?

Before access is denied, read and review the requirements and explanations under "Does a patient have access to his/her entire PHI?" (Mentioned earlier in this policy.)

Once access is denied, the patient must be provided a written explanation that meets these requirements:

- It must be written in plain language.
- It must explain why the request is being denied.

If the denial is reviewable, then the patient's right to appeal the decision must be included. For information on what is reviewable, see the following section, "What if a patient disagrees with the denial?"

The denial must include a description of how patients/representatives can file complaints, including the name, or title, and telephone number of a contact person.

Additionally, if access is denied because you do not maintain the requested PHI, but you or CFBHN generally knows where it is maintained, you must notify the patient.

Finally, if some, but not all, of the information can be provided to the patient/representative, then you must provide access to the available information. In some cases, you may deny access to only parts of the requested PHI.

What if a patient disagrees with the denial?

Patients can appeal the denial for access to PHI by submitting a written request for a review of the denial. CFBHN must identify a licensed health care professional who has been assigned as the reviewing official. This person must not be involved in the original decision to deny access. According to the requirements, the assigned health care professional will evaluate all of the information available and make a decision on the appeal within a reasonable amount of time. In the federal Rule, reasonable amount of time is not defined, but the original determination for access is limited to 30 days.

According to the Rule, some denials are not reviewable; therefore, a formal review is not required. The reviewing official does not review the following denials:

- Psychotherapy notes;
- Information collected for use in a civil, criminal or administrative action or proceeding;
- PHI maintained by an organization covered under the Clinical Laboratory Improvements Amendments of 1988 (42 USC 263a) or that is specifically exempt from these Amendments (42 CFR 493.3(a)(2));
- The patient requesting copies of PHI is a correctional facility inmate;
- Information obtained during the course of research, as long as the research is still occurring;
- Records subject to the Privacy Act (5 USC 552a);
- Under a promise of confidentiality, information is obtained from someone other than a health care provider.

AUTHORITY

45 CFR §164.524 (2002)
45 CFR §164.310 (2002)

8. Patient's Right to Request Privacy Protection

PURPOSE

This policy explains the process patients use to request restrictions on the use or disclosure of PHI.

POLICY

8.1. CFBHN will recognize the patient's right to request restriction of uses and disclosures.
§164.522(a)

8.2. CFBHN will recognize the patient's right to request confidential communications.
§164.522(b)

8.3. CFBHN will document the restriction.
§164.530(j) and §164.522(a)(3)

PROCEDURES

CFBHN must allow patients to request restrictions on uses or disclosures of PHI except as needed for treatment, payment or health care operations and for involvement in the patient's care and notification.

CFBHN must also allow patients to request confidential communications from CFBHN.

PHI Restrictions

When patients/representatives ask to have restrictions placed on the use and disclosure of their PHI, you must follow these procedures.

Provide a Protected Health Care Information Restriction Request Form

Have the Patient fill out the *Request to Restrict Uses and Disclosures of Protected Health Information* form used by CFBHN. Assist the patient in filling out the form, if necessary (§164.522(a)(1)). Do not ask the patient's purpose for requesting the restrictions.

Immediately give the request to the Privacy Officer.

Privacy Officer Responsibilities

The PHI restriction and scope of the request

a. Discuss the scope of the request with the patient. In the following instances, the request may not be honored:

- For the patient's emergency treatment, disclosures may be made to another

health care provider (§164.522(a)(1)(iii)). Explain that if information is released for emergency treatment CFBHN will request that the information not be used or disclosed for any other purpose (§164.522(a)(1)(v)).

- The Secretary of the Department of Health and Human Services is to insure that CFBHN is in compliance with these regulations (§164.502(a)(2)(ii)).

- A listing in a CFBHN directory of individuals in its facility, unless the individual expresses specific objection (§164.510(a)).

- Instances where patient authorization or agreement to disclosure is not required are those with purposes that are:

    - By law;
    - By public health activities;
    - About victims of abuse, neglect or domestic violence;
    - For health oversight activities;
    - For judicial and administrative proceedings;
    - For law enforcement purposes;
    - Regarding decedents;
    - For organ donation;
    - For research purposes;
    - To avert serious threat to health or safety;
    - For specialized government functions;
    - For workers' compensation.

b. Determine restrictions being requested.

   Using the criteria explained above, check to make sure there is no reason to deny the requested restriction. If there is no reason to deny the request, complete the *Response to Request to Restrict Uses and Disclosures of Protected Health Information* form. This should be returned to the patient for confirmation, and should also be placed in the record.

   If the request cannot be honored, explain the reasons on the form for the patient's knowledge and for documentation in the patient's file.

Reasons to Terminate a Restriction

a. If the patient agrees to, or requests, in writing that the restriction be eliminated, (§164.522(a)(2)(i)) place the written request in the patient's record.

b. If the patient orally requests or agrees that the restriction be terminated, the oral request must be documented (§164.522(a)(2)(ii)). Enter the date, and the name of the person agreeing to terminate the restriction, and place in the patient's file. Be sure you sign all documentation.

c. If you want to terminate an agreement to restrictions, give the patient written notice that you are terminating the agreement (§164.522(a)(2)(iii)). Information received during the time the agreement was in effect continues to be restricted. New information (after termination of the agreement) is not restricted by the original agreement.

Document

a. You must maintain written documentation or an electronic copy of all actions taken regarding PHI (§164.530(j)).

b. Maintain documentation for six (6) years from the date of creation or the date when it was last in effect, whichever is later (§164.530(j)).

c. When releasing restricted information, send the *Non-Disclosure Statement for Emergency Treatment* form along with the information, and place a copy in the patient's record.

Confidential Communications

A patient may request that information be provided in an alternative format or at an alternate location. Have the patient complete a *Request for Confidential Communications* form. In these instances utilize the following criteria:

a. You may require requests for alternative means of communication to be made in writing (§164.522(b)(2)(i)).

b. You may *not* require the patient to provide a reason or explanation for requesting confidential communication (§164.522(b)(2)(iii)).

c. When a patient requests communication of PHI, you should complete a *Response to Confidential Communications* form for the patient. Provide the information at the location and in the format most preferred by the patient, if it is reasonably possible for CFBHN to do so (§164.522(b)(1)). The patient must specify an alternative address or method of contact (§164.522(b)(2)(ii)(B)).

d. If you have reason to believe that a request could endanger the individual, you may require that the written request contain a statement that disclosure of all or part of the information requested could endanger the individual (§164.522(b)(2)(iv)).

FREQUENTLY ASKED QUESTIONS

How do patients request restrictions?

Patients have the right to request restrictions on the use and disclosure of PHI. CFBHN provides a form to patients to request restrictions. CFBHN will help patients complete the form, if

necessary. Patients can request restrictions to the use and disclosure of their PHI, or they can request confidential communications.

What is a restriction on the use and disclosure of patient PHI?

Patients may request a restriction on the way their PHI is used or disclosed. For example, a patient with a medical condition, for example, may request that the diagnosis not be disclosed.

What is confidential communications?

Patients may request confidential communications from their doctor's office; this means that all communication about such patient's PHI must be kept confidential. Patients may request that all PHI be sent to post office boxes instead of their home addresses, or they may request that phone calls be received at a different number.

Do I have to agree to a requested restriction?

No, you are not required to agree to a requested restriction, but if you deny the request, you must explain the reasons to the patient.

What happens if emergency treatment is necessary and I have agreed to a restriction?

If the individual requesting the restriction is in need of emergency treatment and PHI is needed to provide the emergency treatment, you may use or disclose the information necessary to provide the emergency treatment. If you release restricted information, you must receive assurance that the recipient of this information will not use or disclose the information except as necessary to treat the patient.

Once a restriction is put in place can it be terminated?

Restrictions can be terminated at the patient's request and, whenever possible, should be in writing. Oral requests can be granted, but the requests must be documented in the patient's record.

If you wish to terminate restrictions, you must notify the patient in writing. You must continue to restrict information received during the initial agreement, but information received after the termination does not have to be restricted.

AUTHORITY

45 CFR §164.522 (2002)
45 CFR §164.530(j) (2002)

9. Patient's Right to Amend Protected Health Information (PHI)

PURPOSE

The purpose of this policy is to explain a patient's right to amend PHI, and what steps CFBHN must take to make or deny the request for amendment.

POLICY

9.1. CFBHN will recognize the patient's right to request an amendment to PHI.
§164.526

9.2. CFBHN will respond to requests to amend PHI within sixty (60) days. If CFBHN requires more time to process a request, the patient must receive notice.
§164.526(b)

9.3. CFBHN will accommodate the patient's right to disagree with any denial of a request for amendment to PHI, and will document this disagreement if further requested.
§164.526(d)

9.4. CFBHN will document the request to amend PHI and subsequent action.
§164.530(j) §164.526(f)

PROCEDURES

Request for Amendment to PHI

A patient has a right to request amendment to his or her PHI. You may require that patients make their requests in writing and provide a reason for the amendment in their requests. Use the form, *Request to Amend PHI*, to allow patients to make such requests.

Additionally, if you receive notice from another covered entity regarding an amendment to a patient's PHI, you must document the affected PHI in your records.

Unable to Act on the Request for Amendment
§164.526(c)

Once a patient requests an amendment you must act on the request within 60 days. If you are unable to act within the required time, you may extend the time to include another 30 days. CFBHN can have only one extension per amendment request.

You must provide a written statement to the patient with the reasons for delay and the date by which CFBHN will complete action. Use the form, *Extension of Time to Respond to Request to Amend PHI,* to provide the required written statement.

Granting the Request for Amendment
§164.526(c)

If CFBHN decides to grant the amendment request, you must proceed to amend the information as requested. You may decide to make the amendment request in whole or in part. Use the form, *Response to Request to Amend PHI* to provide the required response.

To amend a record, you must:

a) Identify the affected records.

b) Make the amendment as requested in every identified record, or provide a link to the appropriate location of the amendment.

c) Inform the patient that the amendment has been accepted. Use the form, *Response to Patient Request to Amend PHI* to provide the required written statement.

d) Ask the patient to identify other persons or organizations that use this PHI. Ask the patient for written authorization to share the amendment. Use the form, *Response to Patient Request to Amend PHI* to provide the required written statement.

e) CFBHN must make a reasonable attempt, within a reasonable time frame, to provide the amendment to those people identified by the patient.

f) CFBHN must also attempt to inform Business Associates or partners who use the PHI that has been amended.

Denying the Request for Amendment
§164.526(d)

CFBHN may deny a patient's request for an amendment if:

- The PHI was not created by CFBHN. However, if you did not create the PHI, but the organization or person that did create the PHI is no longer available to amend the PHI, then CFBHN may choose to make the amendment.

- The PHI is not part of the designated record set (the medical records CFBHN maintains on the patient).

- The PHI would not be available for inspection under our "patient's right to access policy" (written to conform to the HIPAA law §164.524). This section of the law states that psychotherapy notes, information compiled in anticipation of, or for use in a civil, criminal or administrative action or proceeding, information subject to the Clinical Laboratory Improvements Amendments; or information specifically exempt from the Clinical Laboratory Improvements Amendments, are not available for inspection.

- CFBHN believes that the PHI is already accurate and complete.

If the amendment is denied in whole or in part, you must provide the patient a written explanation of the denial. The explanation must include:

a) Plain, understandable language;

b) The basis for the denial;

c) A statement of the patient's right to submit a written statement disagreeing with the denial and instructions on how to file the complaint (CFBHN may reasonably limit the length of the statement of disagreement);

d) A process for patient complaints to CFBHN(include the name, or title, and telephone number of a contact person);

e) A description of how a patient may complain to CFBHN or to the Secretary of the Department of Health and Human Services.

Use the form, *Response to Patient Request to Amend PHI* to provide the required response.

After an Amendment has been Denied

Preparing a Rebuttal Statement
§164.526(d)(3)

After you have denied a patient's request for an amendment, the patient may submit a *Response to Request for Amendment.*

CFBHN may prepare a written rebuttal to the patient's statement of disagreement. If you do, you must provide the patient with a copy of your rebuttal.

Future Disclosures
§164.526(d)(3)

If the patient filed a statement of disagreement, you must always disclose with the PHI that is the subject of the request, the request for amendment, the denial of the request, the statement of disagreement, if any, and CFBHN's rebuttal, if any. You may elect to attach a summary of the request, denial, disagreement and rebuttal.

If the patient did not file a statement of disagreement, you do not have to include the request for amendment or denial with future disclosures unless the patient has requested that they be included. If requested by the patient, you must enclose with any future disclosures of PHI, the request for amendment and the denial of the request. You may elect to attach a summary of the request and denial.

If the disclosure is a standard disclosure that may occur automatically, you may forward this additional information under separate cover.

Record Keeping
§164.526(d)(4)

If a request for an amendment has been denied, you must identify the affected PHI, and record the following information with that original record, or provide a link:

- The patient's request for an amendment;
- CFBHN's denial of the request for amendment;
- The patient's statement of disagreement, if any;
- CFBHN's rebuttal statement, if any.

FREQUENTLY ASKED QUESTIONS

How do patients request amendments?

You may require that patients request amendments to PHI in writing.

How long do I have to act on an amendment request?

You must either grant or deny a patient's request to amend PHI within 60 days. If more time is needed, you may use an additional 30 days, as long as you provide written notification to the patient. This notification must explain why the additional time is needed and must provide the date by which action will be taken on the request.

What do I do if a request is granted?

If a request is granted, you identify the affected records and amend or append the information, or provide a link to the location of the amendment.

You must inform the patient that the amendment has been accepted and request that the patient identify others who need to be informed of the amendment. You should make reasonable attempts to notify others who need to be informed of the amendment.

What do I do if a request is denied?

If a request is denied, you must provide written notice to the patient. Your explanation should include the reasons for the denial and explain the patient's rights and processes for disagreement.

AUTHORITY

45 CFR §164.526 (2002)
45 CFR §164.526(b) (2002)
45 CFR §164.526(d) (2002)
45 CFR §164.530(j) (2002)
45 CFR §164.526(f) (2002)

10. Patient's Right to an Accounting of Disclosures of Protected Health Information (PHI)

PURPOSE

This policy explains the process for providing patients an accounting of their PHI disclosures.

POLICY

10.1. CFBHN will recognize the patients' rights to request an accounting of disclosures of their PHI.
§164.528

10.2. CFBHN will prepare the accounting of disclosures of PHI with content that meets requirements as described in the procedures created by CFBHN.
§164.528(b) and (c)

10.3. CFBHN will document the request for an accounting of disclosures of PHI and subsequent action.
§164.530(j) and §164.528(d)

PROCEDURES

Patient Requests Accounting of PHI Disclosures
§164.528

Print the *Request for Accounting of Disclosures* form and ask the patient to complete and sign the form. Give the form to CFBHN's Privacy Officer. The Privacy Officer must:

Determine if the patient has made an accounting request in the last 12 months. If so:

- Notify the individual that a fee will be charged to generate the accounting.
- Tell the patient that if payment is declined the request for an accounting of PHI disclosures will be terminated.
- Tell the patients that they have the opportunity to modify their requests so as to reduce fees.

Note: You cannot charge fees to a patient who is requesting an accounting of disclosures for the first time in any 12-month period.

Determine if the accounting is permissible. A patient cannot request an accounting for the following purposes:

- PHI used or disclosed for the treatment, payment or health care operations of the patient.
- Disclosures that were made to the patient.
- Disclosures that were made with written authorization from the patient.

- Incidental disclosures, such as two doctors discussing a patient's case in the hospital hallway, which may have been overheard.
- Disclosures of PHI included in a facility directory.
- Disclosures made for national security or intelligence purposes.
- Disclosures to law enforcement or correctional institutions.
- Disclosures made as part of a limited data set.
- Disclosures that were made prior to the HIPAA compliance date.
- Disclosures that were made more than six years before the date of the request for an accounting.

Determine if the accounting can be provided to the individual within 60 days of the request. If not:

- Print and complete the *Extension of Time for Accounting of Disclosures* form. You are allowed a 30- day extension. You must provide the estimated time the accounting will be available, and a reason for the delay. CFBHN is allowed only one extension per request for accounting of disclosures.
- Send the completed form to the individual.

Providing The Accounting of Disclosures

a. Check to be sure that there are no active written or documented "suspensions of disclosure rights" on file that fall within the time period covered by the disclosure accounting request. If there are, be sure to EXCLUDE this information from the accounting of disclosures.

b. Print out and complete the Response to Request for Accounting of Disclosures form.

c. Gather and record the disclosure information for the requested period not to exceed the six years prior to the request, and does not cover the period prior to April 14, 2003. This information may include PHI from other providers.

d. Provide any support documents required for the accounting.

e. Send the patient the accounting, which includes:

- Date;
- Name of recipient of PHI and address, if known;
- Brief description of PHI;
- Brief statement of purpose, or a copy of the request for PHI.

f. For multiple disclosures sent to the same person for the same or similar purposes, send the above information and include the frequency, periodicity, and number of requests, as well as the date of last disclosure. You are not required to provide copies of each of these disclosures.

g. For disclosures of PHI made for research purposes involving 50 or more people,

CFBHN can prepare a statement for all of its patients requesting an accounting. The statement should state that the patient's PHI may have been included, and must also include:

- The name of the protocol or other research activity.
- A description of the research, including the purpose of the research and the criteria for selecting records.
- A brief description of the PHI that was disclosed.
- The date or period of time for the disclosure, including the last date a disclosure was made for this purpose.
- The name, address or telephone number of the entity that sponsored the research, and the researcher who received the information.

If it is reasonably possible that patients were a part of this research, then, at the request of the patients, you must help them locate the sponsor of the research.

File a copy of the PHI disclosure accounting and other required information in the patient's file. Your documentation must include the information that you provided and the title of the persons or offices responsible for receiving and processing requests for accounting by patients. This information must be retained for no less than six years from the date the accounting was made.

CFBHN must document the disclosures that are required by law to be included in the accounting, and the written accounting that is provided to the patient.

Suspension of an Individual's PHI Disclosure Accounting Rights
§165.528

Written Request

Verify that the written statement includes notification that the accounting to the individual would be reasonably likely to impede the agency's activities and specifies the time for which such a suspension is required.

Oral Request

Document the oral request. Include the identity of the agency or official making the request. If an oral request is made, it can last no more than 30 days from the date of the request. If the health oversight agency or law enforcement official would like to extend this time period, they must submit a written request.

CFBHN's Privacy Officer must file the information in the individual's file for consideration when a disclosure accounting request is received from the individual.

FREQUENTLY ASKED QUESTIONS

Who can request an accounting of PHI disclosures?

All patients have a right to receive an accounting of disclosures (a list) of their PHI made by CFBHN in the six years prior to the date the accounting is requested and after April 14, 2003. Most routine disclosures do not have to be reported to the patient, but the patient has a right to receive an accounting, even if no qualified disclosures were made.

How does a patient request an accounting of disclosures?

Patients can make this request at any time, either orally or in writing. CFBHN may choose to require that a patient fill out a *Request for Accounting of Disclosures* form to request an accounting of disclosures.

Be sure to document all requests for an accounting of disclosures with your Privacy Officer.

We have received a request for an accounting of disclosures…Now What?

After you have received a request for an accounting of disclosures, you must act on the request within 60 days from the date you received the request. If you cannot provide the accounting as requested within 60 days, you must provide a *Response to Request for Accounting of Disclosures* form to notify the patient that the accounting cannot be provided within this time frame. This notice must include the reasons for the delay and the approximate date the accounting will be provided. Which can be up to another 30 days from the previous deadline.

Note: CFBHN is only allowed *only* one 30-day extension.

Once information has been prepared, and the accounting of disclosures is provided, you must document the disclosure. You should record in the patient's file what information was disclosed, to whom, and the date.

Do we have to prepare an accounting of ALL disclosures of PHI?

CFBHN must include all disclosures of PHI that CFBHN has made that are not accompanied by a signed release of information made in the time frame specified in the request. A patient may request an accounting for up to six years prior to the date of the request, as long as the six years occurred after the HIPAA compliance date. For example, you would not provide an accounting of disclosures that were made prior to April 14, 2003, the HIPAA compliance date.

Most disclosures of PHI are exempt from this accounting. They are disclosures made for:

- Treatment, payment, or health care operations.
- The patient.
- A facility directory, or for notification purposes.
- National security or intelligence.
- Correctional institutions or law enforcement officials.
- Part of a limited data set (disclosures that did not reveal patient name or ID).

What must be included in the accounting of disclosures?

CFBHN must provide the patient with a written accounting of disclosures. This document must include all of the following:

- The date of the disclosure.
- The name of the person or organization that received the PHI.
- The address of the person or organization that received the PHI, if known.
- A brief description of the PHI that has been disclosed.
- A brief statement of the purpose of the disclosure.

If you repeatedly disclose PHI to the same person or the same entity for the same reason, you can consolidate the accounting by providing all the above information, and include:

- The frequency of these multiple disclosures.
- The last date of the disclosure.

If you have made a disclosure of PHI for purposes of research for 50 or more patients, you must provide to the patient:

- A protocol of the research.
- A brief description of the purpose of the research.
- A brief description of the PHI disclosed.
- The date or time period for the disclosure.
- The name, address, and telephone number of the entity that sponsored the research and of the researcher who received the PHI.
- A statement that the PHI of the patient making the request may or may not have been included in this disclosure.

Can we charge a patient for the Accounting of Disclosure?

CFBHN is obligated to provide every patient a free accounting of disclosures within any twelve-month period. In other words, each patient can request one disclosure each year. After that, CFBHN may charge a reasonable cost-based fee for the preparation. The patient must be informed of the fee in advance, and given the opportunity to modify or rescind their request.

AUTHORITY

45 CFR §164.528 (2002)
45 CFR §164.528(b) and (c) (2002)
45 CFR §164.530(j) (2002) and 45 CFR §164.528(d) (2002)

11. Patient's Right to Assign a Personal Representative and Rights of Emancipated Minors

PURPOSE

This policy explains how patients can assign representatives to authorize health care services.

POLICY

11.1. CFBHN recognizes the patient's right to assign a personal representative, and will treat the personal representative as the patient.
§164.502(g)

11.2. CFBHN recognizes the rights of emancipated minors and will treat them as the adult patient.
§164.502(g)(2) and (3)

PROCEDURES

Assigning a Personal Representative

Personal Representative
§164.502(g)

A patient may have a personal representative, and the representative must be treated just as the patient would be treated by CFBHN. This means that the personal representative can receive PHI about the patient, is able to make written authorizations for disclosure just as the patient would, and can make medical decisions for the patient.

Verify the Personal Representative

If someone claims to be the personal representative of a patient, you must first confirm his or her authority to act on behalf of the patient.

Adult or Emancipated Minor

If a person has legal authority to act on behalf of an adult or emancipated minor in making decisions related to health care, CFBHN must recognize this person as the patient's personal representative.

CFBHN may request written documentation, such as a court order, that the person has legal authority. CFBHN should make a copy of this documentation for the patient's file for future reference. For example, you will need such verification if the person requests the patient's PHI.

Unemancipated Minor

If a parent, guardian, or other person acting *in loco parentis* has authority to act on behalf of a minor, then CFBHN must recognize that person as the personal

representative of the patient.

CFBHN may request evidence of the representative's relationship to the patient. For example, if the person is the patient's parent, you may ask for a picture identification to confirm the parent's name and identity. If the representative is the legal guardian, you can ask for written documentation. CFBHN should make a copy of this documentation for the patient's file for future reference. For example, you will need such verification if the person requests the patient's PHI:

Exceptions Under Law

There are some exceptions under law where unemancipated minors may make their own decisions regarding health care.

- A minor has the authority to act as an individual with respect to health information and health care service in certain circumstances prescribed by law. The consent of the unemancipated minor in this case is sufficient.
- A minor may lawfully obtain health care services without the consent of a parent or guardian, if a court or another person authorized by law gives
- A parent or guardian may allow for an agreement of confidentiality between a covered health care provider and the minor with respect to health care services.

Representative of Deceased Individual

If an executor, administrator or other person has authority to act on behalf of a deceased person or that person's estate, CFBHN must recognize that person as the personal representative of the deceased patient.

CFBHN may request documentation necessary to verify the person's legal status as the deceased patient's personal representative. CFBHN should make a copy of this documentation for the patient's file for future reference. For example, if the person requests additional information on the patient, you will need this verification.

Verify the Circumstances

After you have confirmed that individuals are authorized to serve as patients' personal representatives, and before you allow them to see PHI or make medical decisions, you should verify the circumstances. There are some circumstances when access to PHI can be denied.

Abuse, Neglect or Endangerment

CFBHN may elect not to treat a person as the personal representative of a patient, if any of the following apply:

- You have a reasonable belief that the patient has been or may be subjected to domestic violence, abuse, or neglect by the person acting as the personal

representative.
- You have a reasonable belief that treating the person as the personal representative could endanger the patient.

Existing State or Case Law

Existing State or other law, including applicable case law, may require that you disclose the PHI of an unemancipated minor to a parent, guardian or other person acting *in loco parentis*, regardless of whether or not they are the patient's personal representative. You must act in compliance with applicable State or other law.

Existing State or other law, including applicable case law, may prohibit the disclosure of the PHI of an unemancipated minor to a parent, guardian or other person acting *in loco parentis*. You must act in compliance with applicable State or other law.

When the parent, guardian, or *loco parentis* is not the personal representative of the unemancipated minor patient, and state law or other applicable case law does not prescribe access, CFBHN may decide whether or not to disclose PHI. This decision must be made by a licensed professional using his or her professional judgment.

Patient Interest

You may deny access to PHI if, in the exercise of professional judgment, you decide that it is not in the best interest of the patient to treat the person as the patient's personal representative.

Once you have verified the authority of the personal representative and the individual circumstances, CFBHN must recognize the personal representative as the patient.

FREQUENTLY ASKED QUESTIONS

What is a personal representative?

A personal representative is an adult who has been assigned as a patient's delegate for health care services. A personal representative can speak to medical professionals about the patient, make decisions regarding the patient's health care, and can view and use PHI. You should treat the personal representative as the patient.

Who can have a personal representative?

An adult or an emancipated minor patient may choose to assign a personal representative. Furthermore, a minor will need a personal representative and, in most cases, this will be the minor's parent or legal guardian. However, it may be necessary for a court to authorize someone, other than a parent, to serve as the personal representative. This may include foster parents, shelter providers or state welfare officials appointed by the court.

Deceased patients may have a person who is authorized to handle their estate, such as an

executor or estate administrator, and serve as the decedent's personal representative.

What if the personal representative is not benefiting the patient?

There might be some situations where, in your professional judgment, the personal representative is endangering the patient. You may choose not to disclose PHI to a personal representative if:

- You have reasonable belief that the patient has been or may be subjected to domestic violence, abuse, or neglect by the person acting as the personal representative.
- You have a reasonable belief that treating the person as the personal representative could endanger the patient.
- In your professional judgment, you believe that the personal representative is not acting in the best interest of the patient.

AUTHORITY

45 CFR §164.502(g) (2002)

12. Privacy Records and Compliance Reports

PURPOSE

In order to enforce the requirements of Federal Privacy Regulations, the Secretary of the Department of Health and Human Services (HHS) may periodically audit CFBHN for compliance, and investigate complaints and appeals from CFBHN patients. Therefore, CFBHN must make all of its records, including Protected Health Information (PHI), available to HHS and cooperate with all other HHS requests.

POLICY

12.1 CFBHN will provide records and compliance reports to the Secretary of the Department of Health and Human Services. §160.310

12.2 CFBHN will permit access to protected health information to the Secretary of the Department of Health and Human Services. §160.310(c)

PROCEDURES

Records and Compliance Reports
§160.310

A representative of the Secretary of the Department of Health and Human Services (Secretary) may require information to ascertain whether CFBHN has complied, or is complying with the Privacy Rule. CFBHN must cooperate with the Secretary if the Secretary undertakes an investigation or compliance review of the policies, procedures, or practices of CFBHN.

If you receive a request for information, you must give it to CFBHN's Privacy Officer. A form is not required for this procedure.

It is the responsibility of the Privacy Officer to ensure that CFBHN:

- Provides full cooperation with HHS representatives.
- Allows access to information during normal business hours. This includes facilities, books, records, accounts, and other sources of information.
- If the Secretary determines that exigent circumstances exist, CFBHN must permit access at any time and without notice.

If any information requested by HHS is in the exclusive possession of another person or organization, CFBHN must attempt to gather that information. If that person or organization is not cooperating, you must document the dates of the requests and the persons or organization's refusal to cooperate.

Record Keeping
§160.310 and §164.530(j)

CFBHN's Privacy Officer must maintain policies and procedures, written communication required by the Privacy Rule, and actions that are required to be documented by the Privacy Rule, in written or electronic form for six years from the date of its creation or from the effective date, whichever is later.

FREQUENTLY ASKED QUESTIONS

Why would HHS need to see CFBHN's PHI?

Since the subject of audits and investigations may pertain to PHI and how CFBHN handles PHI, HHS may need to examine PHI records directly.

Should CFBHN make a Minimum Necessary determination regarding the information HHS is given? Should CFBHN withhold any PHI requested by HHS?

No to both questions. HHS is legally authorized to obtain any information it needs to perform its duties. Because of the nature of HHS audits and investigations, HHS might not give CFBHN reasons for requesting the information. It would be impractical for CFBHN's workforce members to determine the minimum amount of information needed by HHS.

Note: HHS workforce members are under the same obligations as CFBHN workforce members to protect the privacy of CFBHN's patients.

Should CFBHN simply provide everything in response to an HHS request, no matter what the request is?

You can negotiate with HHS regarding the amount, type, and format of the information to make the process easier for both HHS and CFBHN. For example, HHS might choose to specify the minimum necessary information they need in order to help simplify the effort.

Will CFBHN have plenty of prior notice when HHS makes a request?

Not necessarily. In extreme cases, HHS could arrive unannounced (even after business hours) during an investigation. In most circumstances, however, the requests and your responses will occur during the business day and allow reasonable time to gather the information.

What if the information is not under CFBHN's control, for example, it is held off-site by a Business Associate and the Associate is uncooperative with our efforts to respond to HHS' request?

Document your requests to the Business Associate, and, if the Associate is uncooperative, document that as well. When you believe a Business Associate is being uncooperative with CFBHN's efforts to meet an HHS request, immediately inform HHS and provide HHS the documentation.

AUTHORITY

45 CFR §160.310(2002)
45 CFR §160.310(c)(2002) and 45 CFR §164.530(j)(2002)

13. CFBHN's Administrative Actions Regarding Protected Health Information (PHI)

PURPOSE

This policy explains certain administrative actions that CFBHN must take in order to protect a patient's personal information, and to comply with the federal HIPAA regulations.

POLICY

13.1 It is the responsibility of CFBHN to identify covered and non-covered functions, and health care components in recognition of privacy requirements.

13.2 CFBHN will designate a Privacy Official responsible for maintaining policies and procedures to protect the privacy of patient information.
§164.530(a)

13.3 CFBHN will designate a contact person or office responsible for receiving complaints, and for publishing the Notice of Privacy Practices.
§164.530(a)

13.4 CFBHN will create a means for patients to complain about the CFBHN's privacy policies and practices. CFBHN will document all complaints.
§164.530(d) and (j)

13.5 CFBHN will provide training to members of its workforce on the policies and procedures with respect to PHI.
§164.530(b)

13.6 CFBHN will institute appropriate administrative, technical, and physical safeguards to protect the privacy of PHI.
§164.530(c)

13.7 CFBHN will apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of CFBHN.
§164.530(e)

13.8 It is the policy of CFBHN to mitigate, to the extent practicable, any harmful affect known by CFBHN, when disclosing or using PHI.
§164.530(f)

13.9 It is the policy of CFBHN to refrain from any intimidating or retaliatory acts against individuals or groups that may exercise their privacy rights as described in CFBHN policies and procedures.

§164.530(g)

13.10 CFBHN will develop procedures to make changes to the privacy policies and procedures as required by changes in law, changes in the Notice of Privacy Practices, or by CFBHN. §164.530(i) and (j)

PROCEDURES

This policy describes the administrative actions that must be taken by CFBHN to be in compliance with the Privacy Regulations.

Personnel Designations

Privacy Officer and Contact Person
§164.530(a)

CFBHN must appoint a Privacy Official responsible for the development and implementation of the policies and procedures of CFBHN. See the *Privacy Officer Position Description* for more information. The Director of QI is the designated Privacy Officer.

CFBHN must appoint a contact person or office to receive complaints and provide information about the *Notice of Privacy Practices*. This person may be the Privacy Official.

The positions must be documented, including the position descriptions and identifying the individual(s) or office(s) responsible for these functions.

Other Personnel Assignments and Use Among, and Disclosure to Workforce members
§164.514(d)(2)

The Privacy Officer must categorize CFBHN managers, workforce members, contractors, consultants and Business Associates (workers) by the Protected Health Information (PHI) they need to do their jobs. Below are two options for doing this.

For larger organizations with greater specialization, here are eight suggested categories.

Non-medical Operations - These duties can include (non-invoicing) financial management, purchasing, maintaining CFBHN facilities, supplies and equipment and public relations. Workers who fall exclusively into this category should not have access to any PHI.

Non-Treatment Patient Services –(This does not apply to CFBHN) These duties can include greeting and directing patients and visitors, transporting patients, providing patients with non-health care services (like meals). Workers who fall exclusively in this category should only be given access to PHI such as patient names, addresses, locations within the facility and treatment locations.

Medical and Patient Information Management – These duties can include filing,

maintaining, processing, purging and destroying any type of patient information. Workers in this category will have extensive access to PHI.

Scheduling – (This does not apply to CFBHN) These duties can include making patient appointments, arranging, reserving treatment and testing resources, notifying pharmacies about prescriptions, sending out samples for testing and analysis and accepting (but not examining) test results. Workers who fall exclusively in this category should only be given access to patient names and contact information, location and/or purpose of appointments, test samples and sealed test results.

Collections and Payment Processing – These duties can include invoicing, maintaining accounts receivable data, collections, negotiating payments, payment processing and accepting and paying invoices from other entities for treatment related services. Workers who fall exclusively in this category should only have access to patient names, contact information, account numbers etc. and treatment charge information.

Treatment – (This does not apply to CFBHN) – These duties include any and all medical services to CFBHN patients. These workers extensively create and use the most sensitive PHI.

Compliance and Legal Management – These duties can include ensuring CFBHN compliance with any laws, rules or regulations; managing audit engagements or investigations performed by oversight authorities and helping to represent CFBHN in hearings, adverse actions, or litigation. Workers who fall exclusively in this category must be able to handle a wide range of PHI.

Operational and Executive Management – These duties can include hiring and terminating workforce members and contractors, entering into business arrangements on behalf of CFBHN, establishing CFBHN policies and setting the strategic direction. The amount of PHI handled by these managers is based upon the extent to which they are involved in the other (above) aspects of CFBHN's operations.

For a smaller organization with less specialization among the workers, here are four suggested categories.

Non-medical Patient Services and Operations – (This does not apply to CFBHN) These duties can include (non-invoicing) accounting, purchasing, maintaining CFBHN facilities, supplies and equipment, public relations, greeting and directing patients and visitors, transporting patients, providing patients with non-health care services (like meals). Workers who fall exclusively in this category should only be given access to PHI such as patient names, addresses, and locations within the facility and treatment activities.

Scheduling and Payment Processing – These duties can include making patient appointments, arranging for treatment, reserving treatment and testing resources, notifying pharmacies about prescriptions, sending out samples for testing and analysis and accepting (but not examining) test results; invoicing, maintaining accounts receivable

data, collections and payment processing and accepting and paying invoices from other entities for treatment related services. Workers who fall exclusively in this category should only be given access to patient names and contact information, location and/or purpose of appointments, test samples and sealed test results.

Treatment – (This does not apply to CFBHN) – These duties include any and all medical services to CFBHN patients. These workers extensively create and use the most sensitive PHI.

Compliance, Legal, Information and Executive Management – These duties can include ensuring CFBHN compliance with any laws, rules or regulations; managing audit engagements or investigations performed by oversight authorities and helping to represent CFBHN in hearings, adverse actions, or litigation; filing, maintaining, processing, purging and destroying any type of patient information which can include PHI; and hiring/terminating workforce members and contractors, entering into business arrangements on behalf of CFBHN, establishing CFBHN policies and setting the strategic direction. Because PHI is often a part of or the focus of these activities, and managers may need to be involved in several aspects of CFBHN operations, these workers must be qualified to handle PHI.

The Privacy Officer will categorize all CFBHN workers, individually or by class, into categories. However, some workers can be placed into more than one category (in an extreme example, a sole practitioner may perform duties in every category). The Privacy Officer will also implement practices and safeguards to limit workforce members' access to PHI in accordance with their duties. Examples include modifying CFBHN software to distinguish between the access rights of workers involved in payment processing, scheduling or treatment; securing records in a lockable and/or heavily monitored environment, making sure that workers understand the limitations of their access to PHI and the consequences of exceeding those limitations.

For more information on how to use and share PHI among workforce members, and conforming to the regulatory requirements on minimum necessary standards, see the section in these policies and procedures on minimum necessary.

Training
§164.530(b)

CFBHN must provide training to all members of its workforce on the policies and procedures regarding protected health information. For more information about how to access privacy rule training, see CFBHN's Privacy Officer or the training coordinator.

CFBHN will ensure that training will be provided to current workforce members prior to the compliance date.

CFBHN will ensure that training will be provided to new workforce members within a reasonable amount of time after beginning employment with CFBHN. CFBHN will ensure that training will be provided to workforce members when significant changes are made to

the policies and procedures regarding protected health information.

CFBHN will document the date and workforce personnel participating in each training.

Safeguards

§164.530(c)

CFBHN will provide administrative, technical and physical safeguards to protect PHI. CFBHN must reasonably safeguard PHI from any intentional or unintentional use or disclosure that may violate the Privacy Rule. CFBHN must also reasonably safeguard PHI to limit incidental uses or disclosures that can occur during treatment, payment, and operations.

Here are some useful examples of safeguarding PHI:

Personal Safeguards

Remember that you may be held personally accountable if you mishandle PHI.

For example: if you take PHI home, and leave it where others can see or misuse it, you may be subject to the penalties listed in Chapter One, Section F-3 of the Privacy Law and Procedure Manual, as well as subjecting yourself and CFBHN to a possible lawsuit.

Vocal, Telephone and Voice Mail Safeguards

Workforce members should not talk about an individual's PHI in public areas within the workplace, such as elevators, reception areas, and the cafeteria; or outside of the workplace.

Do not play back voice mail messages while using a speakerphone, because the message may contain PHI that could be overheard by an unauthorized person.

Voice mail should be password-protected. Do not give out voice mail password to any non-CFBHN workforce member, and do not post or keep your password written down where it can be readily found by someone else (especially do not tape it to your desk, side of your computer, or telephone).

Mail and Express Mail Safeguards

Make sure that open mail that contains PHI is not left sitting in a public area or unsecured mailboxes. Incoming mail should be delivered directly to the recipient or picked up from the mailroom by an accountable person in each work unit and kept secure, until it can be distributed to the recipient.

Outgoing mail that contains PHI should leave your office in a sealed envelope. If this is not possible due to specific circumstances, you must take reasonable precautions to safeguard the privacy of the PHI.

Fax Safeguards

When you fax PHI, make sure that it is sent with a cover sheet that includes a confidentiality statement, and call the recipient immediately before and after sending the fax to ensure that it is expected and picked up promptly.

Fax machines should be located in an area where an accountable person can ensure that faxes are kept confidential and can promptly distribute them to the proper recipients. Fax machines should not be located in public areas such as reception areas where visitors can view faxes. Faxes containing PHI should not be posted or pinned to bulletin boards in common areas until someone claims the fax.

Email Safeguards

When you forward or copy an email to someone outside CFBHN, first make sure that it does not contain PHI anywhere in the chain of forwarded emails, unless the individual receiving the email is authorized to use the PHI.

When communicating with more than one individual about their PHI, send separate emails to each person so you do not disclose PHI about one individual to another.

For example, in a recent lawsuit, a drug company sent out a reminder email to patients who receive antidepressants to renew their prescriptions. The technician sent the email to the patients, but mistakenly listed all the patients on the "To" line. Every patient got the list of several other patients who were also taking antidepressants. The drug company was subject to potential penalties for failing to safeguard PHI.

Access to your email is password-protected through the network log-in screen. Do not share your password with anyone. Do not leave a copy of your password on a piece of paper where it can be easily found (especially do not tape it to your desk, the side of your computer screen, or telephone).

The supervisor of each individual work unit shall be responsible for ensuring that passwords for terminated workforce members are promptly deactivated.

If PHI is contained in an email it must be treated as PHI maintained in any other form.

Computer Safeguards

Electronic files should be saved on a secure computer. Do not save PHI onto your hard drive or to a diskette, unless it is necessary. When information is saved onto your hard drive or a diskette, it is not password-protected and, therefore, not as secure as when you save information on the network. If you do save PHI onto a diskette, follow the same safeguards you would follow as if the PHI was on paper. Be aware that, even after you delete a file from a diskette, the information can still be recovered using the appropriate technology. The only way to ensure the destruction of the information is to physically destroy the diskette.

Access to computers, databases or networks containing PHI should be password-protected. Do not share your password with anyone, and do not post or keep a copy of your password where it can be easily found. The supervisor of each individual work unit shall be responsible for ensuring that an employee's security privileges are promptly terminated, if an employee leaves employment with CFBHN.

Use a screen saver that activates if the computer is not in use for 15 minutes, and requires a password to log back in.

Use the "lock work screen" function to lock your computer when you leave your workstation. The following steps describe how to use this function.

1) Press CTRL-ALT-DELETE buttons on your keyboard simultaneously. Left click the tab "Lock Computer" (or hit the ENTER button).

2) Your workstation is now locked.

3) To unlock the workstation, follow Step 1, and then enter your Network Password.

4) Your workstation is now unlocked.

Be aware of whether or not your computer screen may be easily seen by office visitors. For example, if you use PHI in your daily work, you may want to reposition your computer screen so that it does not face the hallway or office visitors.

Safeguards for PDAs

For Personal Digital Assistants (PDAs), follow the same types of safeguards as you would for a computer. If the PDA contains confidential information, you must safeguard the PDA from being accessed by anyone outside of CFBHN. If your PDA containing PHI is lost or stolen, you should promptly report the matter to your supervisor and to the Privacy Officer.

Office Safeguards

Do not leave papers that contain PHI lying around where unauthorized people can view them.

At the end of the workday, secure all PHI. During non-working hours PHI should be reasonably secured from intentional or unintentional disclosure. Follow the procedures of your individual work unit. For some work units, this may mean locking the PHI in a file cabinet; for others, it may mean locking the office. If you have any questions regarding your work unit's safeguards, consult with your supervisor or the Privacy Officer.

Privacy Officers shall perform a periodic security review of their facilities to identify areas where PHI is not secure, and assist employees in relocating information or equipment, and to develop procedures to prevent unauthorized access to the information. The review should include:

1) Checking the location of fax machines, mail trays, and mail bins;

2) Checking the location of bins for paper waiting to be shredded;

3) Checking the maintenance and custodial procedures; and

4) Checking the record storage procedures.

The HIPAA liaisons or facility managers must send copies of contracts with maintenance, custodial, shredding, copier service, and storage vendors to the Privacy Officer for review and approval.

Safeguards for Using PHI Off-Site

Workforce members who take work home or to meetings off-site must reasonably safeguard PHI from intentional or unintentional disclosure to unauthorized people. This includes family members and guests. PHI that is used off-site should be secured when not in use, such as a filing cabinet or locking briefcase.

Unsecured and audible answering machines should not be used for relaying messages containing PHI.

Disposing of PHI

Documents containing PHI may not be left in an area where they can be viewed by an unauthorized person. Paper documents that do not have to be retained must be shredded prior to disposal.

Electronic media containing PHI that does not have to be retained must be destroyed prior to disposal.

CFBHN Actions

Complaints About the Policies and Procedures
§164.530(d)

If a workforce member or patient has a complaint about the policies and procedures regarding privacy protection, the employee or patient must:

- Complete and sign the *Complaint* form.
- Submit the form to the Privacy Officer.

A workforce member or patient may also file a complaint with the Secretary of the Department of Health and Human Services.

All complaints and responses must be documented and maintained for a period of six years.

Sanctions
§164.530(e)

If a workforce member suspects that another employee of CFBHN has violated the privacy policies and procedures, the employee must immediately report it to the Privacy Officer. If a patient or another person informs CFBHN about a potential violation of the privacy policies and procedures, it must be immediately reported to the Privacy Officer.

CFBHN's Privacy Officer must thoroughly investigate every suspected violation of the policies and procedures. The Privacy Officer will document the reports and the findings of the investigation.

In the event there is a violation of the privacy policies and procedures, CFBHN will apply appropriate sanctions against the employee(s). The Privacy Officer will complete the *Incident Report* Form, including the dates of the investigation, the results of the findings, and the sanction imposed. The Privacy Officer must discuss the violation with the employee, review the policies and procedure(s) that were violated, and have the employee sign the written sanction, acknowledging receipt and understanding. This written sanction must be filed in the employee's records, as well as the privacy records. It must be maintained for six years from the date of the signature.

CFBHN may impose sanctions as deemed appropriate according to the severity of the violation, mitigating circumstances, and the employee's past performance. This may include termination of the employee.

When a patient's privacy rights have been violated, they must be notified of CFBHN's efforts to mitigate any effects of the violation.

CFBHN cannot sanction a workforce member who is a "whistleblower."
§164.530(e)(1) and §164.502(g)

Mitigation
§164.530(f)

CFBHN must mitigate, to the extent practicable, any harmful effect that is known to CFBHN of a use or disclosure of PHI in violation of its policies and procedures or the requirements of the Privacy Rule by CFBHN or its Business Associates.

Any CFBHN workforce member who discovers that CFBHN or a Business Associate has violated the Privacy Rule or CFBHN's procedures, must immediately report the violation to the Privacy Officer, who will coordinate mitigation efforts.

When a patient's privacy rights have been violated, they must be notified of CFBHN's efforts to mitigate any effects of the violation.

Retaliatory Acts
§164.530(g)

CFBHN and its employees are prohibited from intimidating, threatening, coercing, discriminating or taking other retaliatory action against any individual or organization for exercising their rights to privacy of health information and accountability; for filing complaints, or for participating in an investigation, compliance reviews or other proceedings; or opposing any act or practice that the individual or organization believes is unlawful according to the Privacy Rule. Any violation or suspected violation should be immediately reported to the Privacy Officer, using the *CFBHN Complaint* Form. The Privacy Officer must take immediate action to investigate the reported incident(s). If a violation is proven, corrective action will be taken and sanctions will be applied to employees in violation of this policy.

Waiver of Rights
§164.530(h)

CFBHN will not require patients to waive their rights as a condition of treatment or payment.

Policies and Procedures
§164.530(i)

CFBHN will maintain policies and procedures regarding protected health information. These policies and procedures will be maintained in electronic form or in printed form. The Privacy Officer will maintain the policies and procedures in such a manner as to comply with any changes in the law. Changes may be made at any time, provided the Privacy Officer documents them. When there is a material change in the law that causes changes to CFBHN's policies and procedures or *Notice of Privacy Practices*, the changes must be made promptly.

Any time a change is made, you must:

- Confirm that it complies with the HIPAA standards.
- Document all changes to your privacy practices.
- Update the *Notice of Privacy Practices*, if necessary.
- Make the updated *Notice of Privacy Practices* available to patients.

If a change to the policies or procedures requires a change in the *Notice of Privacy Practices*, its contents must also be updated. This change can apply to PHI created or collected prior to the revised *Notice of Privacy Practices* effective date, provided that the original *Notice of Privacy Practices* included a statement reserving CFBHN's right to make such a change. If CFBHN did not reserve the right to modify the *Notice of Privacy Practices*, it is bound by the privacy practices described in the original Notice for information created or collected during that time.

Facility Review

Privacy Officers should perform a periodic security review of their facilities to identify areas where PHI is not secure; assist employees in relocating information or equipment; and develop procedures to prevent unauthorized access to information. The review should include:

- Checking the location of fax machines, mail trays, and mail bins.
- Checking the location of bins containing paper waiting to be shredded.
- Checking the maintenance and custodial procedures.
- Checking the record storage procedures.

Documentation
§164.530(j)

CFBHN will maintain policies and procedures, and any documentation required by the Privacy Rule, in writing or electronic form, for six years from the date of its creation or the date when it last was in effect of the requests and disclosures, whichever is later.

FREQUENTLY ASKED QUESTIONS

What is a Privacy Official?

Each organization affected by HIPAA, including doctors' offices, hospitals, Medicaid programs, etc., is required to have a Privacy Official. The Privacy Official is responsible for seeing that the privacy policies and procedures are adopted and followed. In a small office, this person may also have other responsibilities. In a very large organization, there may be a Privacy Officer with multiple people providing assistance.

In this policy, it is stated that the CFBHN will enforce use and disclosure rules to safeguard PHI. Ensuring that this policy is implemented is the job of the Privacy Official. If there are any questions, or if any issues arise regarding the use of PHI, the Privacy Official will make the final decision.

For more information on the responsibilities of the Privacy Official, see the position description at the end of this policy and procedure.

Who must receive training?

All members of CFBHN's workforce that come into contact with PHI must receive training in the policies and procedures developed by CFBHN to provide security of PHI.

What safeguards must be followed?

CFBHN employees must adhere to administrative, technical and physical safeguards that are designed to protect a patient's PHI. Minimum safeguards are provided in the procedures, and include such things as using a password and login to access a computer, keeping files in a locked room, and restricting the telephone conversations at the front desk where other patients may hear

them. There are more examples in the procedures.

AUTHORITY

45 CFR §164.530(a)(2002)
45 CFR §164.530(a)(2002)
45 CFR §164.530(d) and (j)(2002)
45 CFR §164.530(b)(2002)
45 CFR §164.530(c)(2002)
45 CFR §164.530(e)(2002)
45 CFR §164.530(f)(2002)
45 CFR §164.530(g)(2002)
45 CFR §164.530(i) and (j)(2002)

14. Business Associates

PURPOSE

This policy explains the process for providing disclosures to Business Associates.

POLICY

14.1. CFBHN will recognize the use and disclosure of PHI to Business Associates.
§164.502(e)

14.2. CFBHN will recognize the necessity of executing Business Associate contracts in order to ensure and safeguard PHI.
§164.504(e)

14.3. CFBHN will recognize its role in safeguarding PHI shared with a Business Associate.
§164.504(e)

PROCEDURES

CFBHN may disclose PHI to a Business Associate and may allow a Business Associate to create or receive PHI on its behalf with satisfactory assurance that they will appropriately safeguard PHI.

A Business Associate is a person or organization who performs, or assists in the performance of, a function or activity involving the use or disclosure of PHI. This may be another covered entity or not. Examples include data analysis, claims processing or administration, quality assurance, billing, legal consulting, accounting services, management or financial services.

Using PHI

The Business Associate may use PHI for:

- Treatment, payment and health care operations.
- Proper management and administration of the Business Associate.
- To carry out the legal responsibilities of the Business Associate.

Disclosing PHI

In order for a Business Associate to disclose information, the disclosure must be required by law, or the Business Associate must obtain reasonable assurances.

The Business Associate must obtain reasonable assurances from the person to whom the information is disclosed, that PHI will be held in confidence and used or further disclosed only as required by law.

- The Business Associate must draft a document specifying reasonable assurances.

- The contract must be dated and signed by both parties, and maintained by both parties.

Satisfactory Assurance

If a Business Associate is required by law to perform a function or activity on behalf of CFBHN, CFBHN must obtain (or attempt in good faith to obtain) satisfactory assurances as required by paragraph 164.504(e)(3)(i). Satisfactory assurances must be documented through a written contract or other written agreement. You should use the *Business Associate Contract* form.

Additionally, if an individual or organization provides services to CFBHN, during which time there is the potential that they may access PHI, then a statement of satisfactory assurances should be included in their contract.

a. Draft a document that provides the satisfactory assurances.
b. Send the document to the Business Associate for review and execution.
c. If assurances are not received, document the attempts and the reasons that such assurances cannot be obtained.
d. Be sure the documents are dated and signed.
e. File and retain these documents.

Business Associate Contract

A Business Associate contract is not required if:

- An organization or person is required by law to carry out a function or activity on behalf of CFBHN. CFBHN may disclose PHI as necessary for the person or organization to meet the requirements of the law. However, CFBHN must still attempt in good faith to obtain satisfactory assurances, and if such attempts fail, must document the attempts and reason they failed.
- The disclosure is to a health care provider for the treatment of a patient.
- The disclosure is to a plan sponsor if CFBHN is part of a health plan or HMO.
- The disclosure is to another covered entity that performs a function or activity on behalf of CFBHN as required by law. You must, however, obtain satisfactory assurances.

If CFBHN wishes to enter into a business association, download the sample *Business Associate Contract* and customize the contract for your needs. However, the following requirements, must be met at a minimum, and retained in the contract:

a. The contract must establish the Business Associate's permitted and required uses and disclosures of PHI, consistent with the Privacy Rule. This may also include use of PHI for management and administration of the Business Associate. This

may include providing data aggregation services relating to the health care operations of CFBHN.

b. The contract must specify that the Business Associate will not use or further disclose the information other than as permitted or required by the contract, or as required by law.
c. The contract must specify the use of appropriate safeguards to prevent use or disclosure of the information, other than as provided for by contract.
d. The contract must specify that the Business Associate will report to CFBHN any known use or disclosure of the information not provided for by the contract of which the Business Associate becomes aware.
e. . If the Business Associate discloses any PHI that is received from, created or received by the Business Associate on behalf of CFBHN, to any agents including subcontractors, the Business Associate must ensure that they agree to the same restrictions and conditions that apply to the Business Associate.
f. The contract must require the Business Associate to make available information for patients who request access to PHI.
g. The contract must require the Business Associate to make available information for amendment, and agree to incorporate any amendments to PHI.
h. The contract must require the Business Associate to maintain documentation required to provide patients an accounting of disclosures.
i. The contract must ensure that the associate's internal practices, books, and records relating to the use and disclosure of PHI received from, created, or received by the Business Associate on behalf of CFBHN, are available to the Secretary for purposes of determining CFBHN's compliance with the Privacy Rules.
j. The contract must specify that at termination of the contract, if feasible, the Business Associate will return or destroy all PHI received from, or created or received by the Business Associate on behalf of CFBHN. The Business Associate will not maintain or retain copies (in any form) of such information. If such return or destruction is not feasible, extend the protections of the contract to limit further uses and disclosures.
k. The contract must authorize the termination of the contract by CFBHN, if CFBHN determines that the Business Associate has violated a material term of the contract. You may omit this statement, if it is inconsistent with statutory obligations of CFBHN or the Business Associate.

Memorandum of Understanding

If CFBHN and its Business Associate are both governmental entities, you may enter into a memorandum of understanding with the Business Associate. This document contains terms that accomplish the same objectives as the contract in 3B above. This memorandum must comply with business association rules as stated in §164.504(e).

a. Draft a memorandum of understanding.
b. Send the document to the Business Associate for review and execution.
c. Be sure the documents are dated and signed.

d. File and retain the contract or agreement.

Breach of Confidentiality or Noncompliance

If a covered entity that is the Business Associate of another covered entity violates the satisfactory assurances it provided, it is in noncompliance with the standards and requirements of the Privacy Rule.

Take Action

If CFBHN knows that the Business Associate, or person to whom the Business Associate disclosed information, engaged in a pattern of activity or practice that was a material breach or violation of the written agreement, or CFBHN suspects they are in noncompliance with the Privacy Rule, CFBHN must do the following:

- Take immediate steps to prevent further breaches or violations.
- Take immediate action to mitigate harm caused by the breach or violation.
- Notify the Business Associate of the breach or violation in writing.
- The Business Associate must take action to end the breach or violation and prevent further occurrences.
- Document this process in writing and retain for a period of six years.

Terminate the Relationship

If the Business Associate does not take reasonable steps to cure the breach or end the violation, or if reasonable steps are unsuccessful, you must terminate the contract. CFBHN must:

- Draft a letter to the Business Associate notifying them that you are terminating contract, and indicate the reasons for termination.
- Be sure the notice is dated and signed.
- Send the termination to the Business Associate by certified mail, receipt requested, for proof of receipt.

Report the Problem

If termination is not feasible, you must report the problem to the Secretary of the Department of Health and Human Services. You must:

- Draft a letter to the Secretary outlining the breach or violations.
- Be sure the notice is dated and signed.
- Send the report by certified mail, receipt requested, for proof of receipt.
- File and retain a copy of these documents.

FREQUENTLY ASKED QUESTIONS

Who is included as a workforce member, Business Associate, or representative?

Business associates or representatives used by CFBHN in delivering services are considered Business Associates. For example, a doctor's office using a billing agency or a laboratory for services would be included in this policy. When Business Associates are used, a written contract or agreement must be in place stating that the Business Associate will safeguard PHI, and follow the privacy policies established by CFBHN.

What does it mean to receive, create, use, or disclose PHI?

This refers to how medical information is used. For example, in the course of treating a single patient, a doctor's office may *receive* medical records from the patient's previous physician, or another physician currently treating the patient. All of these physicians are *creating* new files (PHI) that will be *used* to examine or treat the patient. The physicians may *disclose* PHI at the patient's request or through a referral. The federal rules, and the policies of CFBHN, use the phrase "receive, create use or disclose" to cover all possible uses of PHI.

What is a Business Associate?

A Business Associate is any organization or individual who CFBHN works with in the course of conducting business. This may include a laboratory that conducts tests for your patients, or a billing agency that bills patients and insurance companies. For purposes of this policy, your Business Associates may see PHI. You must be careful in making this determination, however. For example, you may not expect your cleaning service to access PHI but, in the course of cleaning, files may be in their view. Therefore, you should consider them a Business Associate.

Note: If you are working with another *covered entity* that must comply with HIPAA and has created its own policies and procedures to maintain PHI, then a Business Associate contract is not necessary.

What is satisfactory assurance?

This policy attempts to ensure satisfactory assurance that your Business Associates will follow the same policies and procedures that your employees do when conducting business. Business associates must guarantee compliance with your procedures to keep PHI secure. This is achieved through a signed contract with each Business Associate.

What should be in the contract?

The contract between CFBHN and your Business Associates should be carefully designed to ensure satisfactory assurance. The contract should contain provisions that:

- State the purpose(s) for Business Associates to use or disclose PHI, and prohibit them from using the information for any other purpose.
- Require the Business Associate to maintain necessary safeguards to ensure that PHI is not

used or disclosed, except as provided by the contract.

- Require the Business Associate to report to you any use or disclosure of PHI that is not provided for in the contract.
- Require the Business Associate to ensure that any of its subcontractors or agents, to whom it provides PHI, will agree to the same restrictions and conditions.
- Require the Business Associate to make available its internal practices, books, and records relating to the use and disclosure of PHI.
- Require the Business Associate, at termination of the contract, to return or destroy all PHI received from CFBHN.
- State that individuals, who are the subject of the PHI disclosed, are intended to be third-party beneficiaries of the contract.
- Provide that the contract may be terminated by CFBHN if you determine that the Business Associate has violated a material term of the contract.

What does the Business Associate have to do?

Business associates must comply with the terms in the contract. If properly drafted, the contract will require that they use and disclose PHI only for the stated purposes, that they keep such information safe and confidential, and that they document any use or disclosure not provided in the contract. The contract will allow for a relationship with a Business Associate to be terminated if any provision of the contract is violated.

Ultimately, your goal is to have Business Associates follow your policies and procedures, thus maintaining the integrity of PHI.

AUTHORITY

45 CFR §164.502(e)(2002)
45 CFR §164.504(e)(2002)
45 CFR §164.504(e)(2002)