# HIPAA Privacy

# and Medical Record

# Policies and Procedures

**XMGN003**
**Complete Revision: 5/1/2013**
**Email Revision: 10/2/2013**

**HIPAA PRIVACY AND MEDICAL RECORD**
**POLICIES & PROCEDURES**

## TABLE OF CONTENTS

**PAGE**

**HIPAA PRIVACY AND MEDICAL RECORD POLICIES & PROCEDURES**

**TABLE OF CONTENTS**

**PAGE**

**HIPAA PRIVACY AND MEDICAL RECORD**
**POLICIES & PROCEDURES**

## TABLE OF CONTENTS

**PAGE**

**HIPAA PRIVACY AND MEDICAL RECORD**
**POLICIES & PROCEDURES**

**SUBJECT: CONFIDENTIALITY**

**POLICY:**
The Administrator with the assistance of the Privacy Designee is responsible for making sure that any patient-identifiable data and health care information, whether paper or computer based, is kept confidential to protect the privacy and security of the information and ensure that information is released according to state and federal guidelines and professional standards.

Confidential information is information documented during the course of a confidential relationship between the patient and the healthcare provider.

**PROCEDURES:**

1. **Employee orientation and training**: This area includes:
   - A. Mandatory completion of in-service program by all Medical Records employees.
   - B. Cooperation from appropriate department managers, offering of in-service education to all staff.
   - C. Active participation in orientation of all new employees.
   - D. All Facility employees are required to sign the Confidentiality Statement. This is placed in the employee's permanent personnel file and reviewed and updated at least annually. It is also updated during any year there is a significant change in job duties of the employee.

## CONFIDENTIALITY STATEMENT

I acknowledge that this statement applies to all members of the workforce of the facility.
I acknowledge that the facility has formally stated in the HIPAA Policies and Procedures manual its commitment to preserving the confidentiality and security of health information, whether it is maintained or distributed in paper, electronic, verbal, or any other medium or format. I understand that I am required, if I have access to such health information, to maintain its confidentiality and security.

I understand that access to health information created, received, or maintained by the facility is limited to those who have a valid business or medical need for the information or otherwise have a right to know the information. I understand that there are many administrative, physical and technical safeguards in place to protect the privacy and security of this health information, and that any attempt to bypass or override these safeguards is a violation of federal and state laws and the privacy and security policies of the facility.

I understand that approved methods and purposes for access to, uses and disclosures of, and requests for, any and all protected health information created, received or maintained by the facility are limited to those described in the HIPAA Policies and Procedures manual's policies and procedures. I further understand that, with the exception of purposes related to treatment, access to, uses and disclosures of, and requests for an individual's health information must, to the extent practicable, be limited to the minimum necessary to accomplish the intended purpose of the approved use, disclosure or request.

I understand that any known or suspected violation of the confidentiality or security of health information must be reported to my immediate supervisor or to the Administrator immediately.

_____

Signature Date

_____

Printed Name

**SUBJECT: HIV/AIDS RECORDS**

**POLICY:**

1. There are certain characteristics that are unique to the Human Immunodeficiency Virus (hereafter referred to as HIV) and Acquired Immune Deficiency Syndrome (AIDS) relationship to informed consent, counseling, confidentiality, testing, education, reporting requirement, disclosure to third parties and nondiscrimination. Information will be released in a way that will promote the best interest of the patient and in such a way that it cannot be used against his/her best interests.
2. The Privacy Designee will have a thorough knowledge of general medical record policies of practice in order to provide sound judgments in issues, which relate to HIV records. This section will attempt to emphasize ONLY those points that are unique to the protection and control of HIV records.
3. **Principles of Confidentiality for HIV and AIDS Records:**
   - A. The intent of the extensive legislation is to encourage voluntary testing. As with all health records, certain principles of confidentiality is automatically assumed and adhered to consistently.
   - B. The identity and test results of any person upon whom a test has been performed are confidential. No person who has obtained or has knowledge of a test result pursuant to this section may disclose or be compelled to disclose the identity or the test results of any person upon whom a test is performed except as provided in the specific release for information pertaining to HIV/AIDS test results.
     1) Test results may be disclosed to the subject of the test or the subject's legally authorized representative.
     2) The identity and test results of any person upon whom a test has been performed may be disclosed to any person, including third party payers, designated in a legally effective, specific release for information pertaining to HIV/AIDS rests results executed prior to or after the test by the subject of the test or the subject's legally authorized representative. The test subject may, in writing, authorize the disclosure of the test subject's HIV results to third party payers, who need not be specifically identified, and to other persons to whom the test subject subsequently issues a general release of medical information, as long as such persons are listed in the specific release.
   - C. Whenever a disclosure is made, it is accompanied by a statement, in writing, which includes the following or substantially similar language:

     "This information has been disclosed to you from records whose confidentiality is protected by state law. State law prohibits you from asking for any further disclosure from the person to whom such information pertains, or as otherwise permitted by state law. A general authorization for the release of medical or other information is NOT sufficient for this purpose."

     **NOTE:** Please remember to verify specific State applicable laws.
   - D. A violation of the above statement by a facility or licensed health care provider will be grounds for disciplinary action by the respective licensing authority.
   - E. A general rule that parental consent is required prior to medical diagnosis or treatment of a minor does not apply when sexually transmitted diseases are involved. Children twelve (12) or older be presumed capable of exercising informed judgments unless facts suggest otherwise are.

**SUBJECT: HIV/AIDS RECORDS (Continued)**

1) A blanket consent for release of information is never to be utilized. A patient gives specific consent for each disclosure initiated. Specific authorization means that the release specifically states that HIV information will be released. Verify with state statutes regarding the procedures for releasing HIV information.
2) Such information is not to be re-released to other third party parties without the specific consent of the patient.

IF THERE IS ANY DOUBT OR CONFUSION REGARDING RELEASE OF HIV INFORMATION, CONSULT THE FUNDAMENTAL ADMINISTRATIVE SERVICES, LLC LEGAL DEPARTMENT FOR ADVICE.

## GENERAL PRIVACY STATEMENT

The facility has a long-standing commitment to protecting the privacy of individually identifiable health information which is sometimes referred to as Protected Health Information ("PHI"). A part of this commitment involves compliance with the privacy policies contained in the regulations promulgated under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the first comprehensive federal protection of health information. This statement generally describes the requirements of the HIPAA privacy regulations. Your facility is referred to as a "Covered Entities" by these regulations and in this statement.

The HIPAA regulations govern the use and disclosure of PHI. In general, a covered entity may use PHI for purposes of treatment, payment, and healthcare operations. It may disclose PHI (1) with the individual's authorization; (2) to another healthcare provider for treatment and payment purposes; and (3) in certain other circumstances described by the regulations.

The HIPAA regulations also give individuals several rights with respect to their PHI. In addition to the right to have access and to receive confidential communications about PHI, the individual may copy and inspect PHI, restrict its use and disclosure, amend it, and receive an accounting of disclosures made of their PHI.

There are many obligations imposed on a covered entity by the privacy regulations. These include developing and implementing policies and procedures to assure compliance; training members of its workforce in the HIPAA requirements appropriate to their jobs; documenting its efforts to achieve compliance; developing and implementing safeguards to protect PHI; and designating a privacy official.

A privacy official is an individual designated by the covered entity who is responsible for the development and implementation of the required policies and procedures for compliance with

HIPAA. The covered entity also must designate a person, who may be the privacy official, to handle complaints and to provide information about the entity's practices with respect to PHI.

The covered entity must provide its patients/residents with a "Notice of Privacy Practices" which explains the patient's/resident's and covered entity's rights and obligations with respect to the use and disclosure of PHI. This Notice must be given to patients/residents at the time the treatment relationship begins.

The effective date of the HIPAA privacy regulation is **April 14, 2003**.

**SUBJECT: DISCLOSURE OF PROTECTED HEALTH INFORMATION (PHI)/MEDICAL RECORDS**

**POLICY:**

1. All information contained in patients'/residents' medical/financial record is confidential.
2. Disclosure of Protected Health Information (PHI) will only be allowed with a properly completed and signed authorization except for the following exceptions:
   A. When required or allowed by law
   B. When the request is:
      1) For continuing care (treatment).
      2) To obtain payment for our services (payment).
      3) For the day-to-day operations of the Facility and the care given to the patients/residents (operations).
      (See *Notice of Privacy Practices* policy for full explanation.)
3. Disclosure of health information will be centralized through the Privacy Designee or his/her designee. The Privacy Designee or his/her designee will need to track releases/disclosures of medical records. This includes vendors or contractors requesting copies of PHI.
4. Disclosure of medical/financial information through the Privacy Designee or his/her designee will be carried out in accordance with all applicable legal, accrediting, regulatory agency requirements and in accordance with written institutional policy.
5. Original medical records are not removed from the premises without approval from the Fundamental Administrative Services, LLC (FAS) Legal Department.
6. The patient has the right to access and obtain copies of his or her PHI. See *Patient's Access to Protected Health Information/Medical Records* policy for additional procedures.

**DEFINITIONS:**

**Protected Health Information (PHI)**: Is defined as individually identifiable health information that is maintained or transmitted by a healthcare provider in any form, including electronic records, paper records and oral discussions. Some examples of protected health information are interdisciplinary progress notes, physician's orders, care plans and billing information that contains patient health information.

**Disclosure:** The release, transfer, provision of access to, or divulging in any other manner of health information.

**For Treatment:** The provision, coordination, or management of health care and related services by the Facility, including the coordination or management of health care by the Facility with a third party; consultation with other health care providers relating to a patient; or the referral of a patient for health care between the Facility and another health care provider.

**Payment:** The activities undertaken by a health care provider or payer to obtain reimbursement for the provision of health care.

**SUBJECT:** **DISCLOSURE OF PROTECTED HEALTH INFORMATION (PHI)/MEDICAL RECORDS (Continued)**

**Health Care Operations:** Any of the following activities of the Facility

1. Conducting quality assessment and improvement activities, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; protocol development, case management and care coordination, contacting of health care providers and patients/residents with information about treatment alternatives; and related functions that do not include treatment;
2. Reviewing the competence or qualifications of health care professionals, evaluating employee and Facility performance, conducting training programs under supervision to practice or improve skills, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;
3. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
4. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the Facility;
5. Business management and general administrative activities of the Facility, including, but not limited to:
   - A. Customer service
   - B. Resolution of internal grievances
   - C. Due diligence in connection with the sale or transfer of assets to a potential successor in interest
   - D. Creating de-identified health information and marketing for which a patient's/resident's authorization is not required.

**PROCEDURES:**

**1. Receiving a Request for Medical Records:**

A. All requests for medical/financial records are referred to the Privacy Designee or his/her designee.

B. The Privacy Designee or his/her designee processes the request and oversees the copying and delivery of the information.

1) All releases are processed through Medical Records.

2) After hours or on weekends, only releases of information for continuing care (i.e., transfer to a Facility or emergency clinic) are permitted. ***See Information Released for Patient Transfer*** policy.

**2. Release Approval**

All requests for medical records are reviewed by the FAS Legal Department. Fax all requests to 410-773-1029.

A. If the request for medical records is not accompanied by an authorization signed by the patient/resident or patient's/resident's legal representative, provide a copy of the Facility's **Authorization to Disclose/Release Information (NFF-IP020P)** form available through DSSI.

**SUBJECT: DISCLOSURE OF PROTECTED HEALTH INFORMATION (PHI)/MEDICAL RECORDS (Continued)**

B. Fax a copy of the request to the FAS Legal Department at 410-773-1029 the day the request is received, utilizing the attached **Fax Cover Sheet**. Be sure to answer all of the questions asked on the cover sheet. Provide copies of all documentation if necessary and communicate any possible concerns.
C. The FAS Legal Department reviews the request to determine whether the request meets the requirements of a HIPAA-compliant authorization, if applicable, and that the requestor is authorized to receive the information under federal and state laws.
D. DO NOT RELEASE copies of any records until you get a response from the FAS Legal Department. You should hear from the FAS Legal Department by the end of the next business day. If you do not receive a response by then, please place a follow-up phone call.
E. Compile the requested records in anticipation of approval by following Step 3, **Preparing the Medical Record for Release**.
F. Once you have **received approval** from the FAS Legal Department to release the medical records, proceed with Steps 4 and 5.

**3. Preparing the Medical Record for Release**

A. The information released is restricted to the information requested.
B. Confirm that the chart is complete.
   1) Are all the consultations, which were ordered in the chart?
   2) Are lab tests, x-rays and other special reports in the chart?
   3) Is the discharge summary in the chart, if applicable?
   4) If any information is missing, locate it and incorporate it into the chart before releasing.
C. Follow the **Exhibit B: Preparing a Medical Record for Release Checklist** once it has been determined that records can be disclosed/copied.
D. When photocopies or other reproductions of health information are provided to authorized external entities, these copies are accompanied by a confidentiality statement; **Exhibit C: Confidentiality Statement**.

**4. Documenting the Release**

A. Log the request in the **HIPAA Correspondence Log** in HIM Department and save the original request documents or authorization in a HIPAA binder or folder. (See **HIPAA Documentation** policy.)

**5. Turnaround Time and Copy Fees:**

A. Requests for photocopies are honored:
   1) When the request is made or authorized by the patient/resident or the legal representative, records must be produced within two working days unless otherwise specified by the requestor or mandated by State la

**SUBJECT:** **DISCLOSURE OF PROTECTED HEALTH INFORMATION (PHI)/MEDICAL RECORDS (Continued)**

2) A fee may be charged for photocopies of medical records as determined by the community policy and State law. If there is no State law, policy is that copies should not exceed $1.00 per page for the first 25 pages and $.25 per page thereafter.
   a) The following individuals are requested to pay for records:
      1). patients/residents or family
      2). attorneys

**6. Responding to Specific Types of Disclosures:**
**NOTE:** See **Request and Reporting Disclosure Table** for information regarding requests by specific entities/individuals.

7. **TELEPHONE REQUESTS:** Notify individuals requesting medical record information via the telephone that they are to submit the request in writing to the Facility.

See Also: Request and Reporting Disclosure Table, Medical Records Request Fax Cover Sheet, Preparing a Record for Release Checklist

**REFERENCE:**

**1. HIPAA Final Privacy Regulations**
45 CFR § 164.504(e)
45 CFR § 164.506
45 CFR § 164.508
45 CFR § 164.510
45 CFR § 164.512

## REQUEST AND REPORTING DISCLOSURE TABLE

| Disclosures to or for: | Is a HIPAA Authorization Required? |
|---|---|
| **Accrediting Agencies (TJC, CARF)** | No, if the disclosure is for health care operations purposes.<br><br>**Need Business Associate Agreement** |
| **Attorney for Patient** | Yes |
| **Attorney for Facility** | No<br><br>**Need Business Associate Agreement** |
| **Avert a Serious Threat to Health or Safety** | Facility may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if Facility, in good faith, believes the use or disclosure:<br>1) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or<br>2) Is necessary for law enforcement authorities to identify or apprehend an individual where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody; or<br>3) Is necessary for law enforcement authorities to identify or apprehend an individual because of a statement by an individual admitting participation in a violent crime that Facility reasonably believes may have caused serious physical harm to the victim, provided that:<br>A) The use or disclosure will not be made if Facility learns of the statement admitting the participation in a violent crime in the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure or through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy; and<br>B) Facility will disclose only the individual's statement admitting the participation in a violent crime and the following protected health information:<br>• Name and address;<br>• Date and place of birth;<br>• Social security number;<br>• ABO blood type and Rh factor;<br>• Type of injury;<br>• Date and time of treatment;<br>• Date and time of death, if applicable; and<br>• 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. |
| **Contractors/ Business Associates** | No, unless their purpose falls outside of treatment, payment or health care operations as defined above. |

| Disclosures to or for: | Is a HIPAA Authorization Required? |
|---|---|
| | **Need Business Associate Agreement** |
| **Coroner or Medical Examiner** | Facility may disclose protected health information 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. |
| **Employer**<br>❑ Requesting healthcare information regarding treatment provided to their employee | Facility may disclose protected health information to an employer, about an individual who is an employee of the employer, if:<br>1) The Facility provides health care to the individual at the request of the employer:<br>A) To conduct an evaluation relating to medical surveillance of the workplace; or<br>B) To evaluate whether the individual has a work-related illness or injury;<br>2) The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;<br>3) The employer needs such findings in order to comply with its obligations to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and<br>4) The Facility provides written notice to the individual that protected health information relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer:<br>A) By giving a copy of the notice to the individual at the time the health care is provided; or<br>B) If the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided. |
| Entity subject to the Food and Drug Administration<br>❑ Adverse events, product defects or biological product deviations<br>❑ Track products<br>❑ Enable product recalls, repairs, or replacements<br>❑ Conduct post marketing surveillance | Facility may disclose protected health information to person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:<br>1) To collect or report adverse events (or similar activities with respect to food or dietary supplements), product defects or problems (including problems with the use or labeling of a product), or biological product deviations;<br>2) To track FDA-regulated products;<br>3) To enable product recalls, repairs, or replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of look back); or<br>4) To conduct post marketing surveillance. |
| **Family members and Individuals Involved in** | For copies of records, the patient's/resident's or legal representative's authorization is obtained. |

| Disclosures to or for: | Is a HIPAA Authorization Required? |
|---|---|
| **Care** | Bills or invoices may be released to the patient's/resident's Responsible Party for payment purposes. See *Definition of Individual Signing Authorization* policy.<br><br>For verbal disclosures, see the policy *Disclosure of Protected Health Information to Persons involved in the Patient's/ Resident's Care*. |
| **Funeral Directors** | Facility may disclose protected health information to funeral directors, consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their duties, Facility may disclose the protected health information prior to, and in reasonable anticipation of, the individual's death. |
| **Healthcare practitioners or Healthcare providers** (hospitals, LTC facilities, home care agencies, DME, pharmacy, EMS/Ambulance Transport, etc.) | No, for continuity of care or payment purposes but a written consent from the patient/resident may be required.<br><br>Yes, if not for treatment or payment purposes. |
| **Health Oversight**<br>❑ Government benefit program<br>❑ Compliance-fraud & abuse<br>❑ Civil rights laws<br>❑ Trauma/Tumor registries<br>❑ Vital statistics<br>❑ Reporting of abuse or neglect<br>❑ Complaint investigation | Facility may disclose protected health information to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for appropriate oversight of:<br>1) The health care system;<br>2) Government benefit programs for which health information is relevant to beneficiary eligibility;<br>3) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or<br>4) Entities subject to civil rights laws for which health information is necessary for determining compliance.<br><br>Exception to health oversight activities. A health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:<br>1) The receipt of health care;<br>2) A claim for public benefits related to health; or<br>3) Qualification for, or receipt of, public benefits or services when a patient's/resident's health is integral to the claim for public benefits or services. |
| **Health Plans/Insurance companies/Third Party** | No, but written consent from the patient/resident may be required. |

| Disclosures to or for: | Is a HIPAA Authorization Required? |
|---|---|
| **Payers**<br>❑ Related to Claims Processing, including determining eligibility, benefits and coverage. | |
| **Judicial and Administrative Proceedings**<br>❑ Court order, court ordered warrant<br>❑ **Subpoena or summons** | Facility may disclose protected health information in the course of any judicial or administrative proceeding:<br>1) In response to an order of a court or administrative tribunal, provided that Facility disclose only the protected health information expressly authorized by such order; or<br>2) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:<br>A) Facility receives satisfactory assurance from the party seeking the information that reasonable efforts have been made to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request. Satisfactory assurances must include a written statement and accompanying documentation demonstrating that:<br>i. the party requesting such information has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);<br>ii. the notice included sufficient information about the litigation or proceeding in which the protected health information is requested to permit the individual to raise an objection to the court or administrative tribunal; and<br>iii. the time for the individual to raise objections to the court or administrative tribunal has elapsed, and no objections were filed or all objections filed by the individual have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.<br>B) Facility receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order. Satisfactory assurances must include a written statement and accompanying documentation demonstrating that<br>i. the parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute~~;~~ or<br>ii. the party seeking the protected health information has requested a qualified protective order from such court or administrative tribunal.<br>A qualified protective order is an order of a court or of an |

| Disclosures to or for: | Is a HIPAA Authorization Required? |
|---|---|
| | administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that prohibits the parties from using or disclosing the protected health information for any purpose other than the litigation or proceeding for which such information was requested; and requires the return to the covered entity or destruction of the protected health information (including all copies made) at the end of the litigation or proceeding.<br>C) Facility makes reasonable efforts to provide notice to the individual sufficient to meet the satisfactory assurance requirements above, or to seek a qualified protective order. |
| Law Enforcement<br>❑ Administrative request<br>❑ Locating a suspect, fugitive, material witness or missing person<br>❑ Victims of a Crime<br>❑ Decedents<br>❑ Crime on Premises<br><br>Contact the FAS Legal Department immediately for guidance. | Facility may disclose protected health information to law enforcement in the following instances:<br>**Required by Law**<br>As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except for disclosures about victims of abuse, neglect or domestic violence, or the reporting of child abuse or neglect.<br>**Administrative Request**<br>In compliance with and as limited by the relevant requirements of:<br>A) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;<br>B) A grand jury subpoena; or<br>C) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:<br>i. The information sought is relevant and material to a legitimate law enforcement inquiry;<br>ii. The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and<br>iii. De-identified information could not reasonably be used.<br>**Identifying or Locating a Suspect, Fugitive, Material Witness, or Missing Person**<br>In response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:<br>A) Facility discloses only the following information:<br>i. Name and address;<br>ii. Date and place of birth;<br>iii. Social security number;<br>iv. ABO blood type and rh factor;<br>v. Type of injury;<br>vi. Date and time of treatment;<br>vii. Date and time of death, if applicable; and<br>viii. A description of distinguishing physical characteristics, |

| Disclosures to or for: | Is a HIPAA Authorization Required? |
|---|---|
| | including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.<br>B) Except ABO blood type and rh factor, Facility may not disclose any protected health information related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.<br>**Victims of a Crime**<br>In response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime except for disclosures about victims of abuse, neglect or domestic violence, or the reporting of child abuse or neglect, if:<br>A) The individual agrees to the disclosure; or |
| | B) The covered entity is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:<br>i. The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the victim has occurred, and such information is not intended to be used against the victim;<br>ii. The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and<br>iii. The disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.<br>**Decedents**<br>For the purpose of alerting law enforcement of the death of an individual if the Facility has a suspicion that such death may have resulted from criminal conduct.<br>**Crime on Premises**<br>Protected health information that Facility believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the Facility. |
| **Life Insurance Carrier** | Yes |
| **Marketing Purposes**<br>❑ Disclosures outside of the Facility for marketing purposes | Yes, with limited exceptions. All Marketing programs involving patients/residents must be approved by the FAS Legal Department. See Marketing Policy |
| Media | Yes, no information is released without the patient's/resident's authorization. |
| **Medicare or Medicaid**<br>❑ Related to Claims Processing, including | No |

| Disclosures to or for: | Is a HIPAA Authorization Required? |
|---|---|
| determining eligibility, benefits and coverage. | |
| **Office of Inspector General (OIG)**<br>❑ Federal<br>❑ State<br><br>**Contact the FAS Legal Department immediately for guidance.** | No, with a subpoena or investigative demand. |
| **Ombudsman** | No, written consent of the patient/resident may be required. |
| **Organ Procurement** | Facility may use or disclose protected health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation where authorized by State law. |
| **Patient** | No, a HIPAA-Complaint Authorization is not required but there must be a written request that is signed by the patient/resident.<br>Not required for viewing of medical records or for information provided verbally to the patient/resident. |
| Patient's Legal Representative | No, a HIPAA-Complaint Authorization is not required but there must be a written request that is signed by the legal representative.<br><br>Not required for viewing of medical records or for information provided verbally to the patient's/resident's legal representative. See *Definition of Individual Signing Authorization* policy. |
| **Public Health Authorities**<br>❑ Reporting of vital events, such as births and death<br>❑ Surveillance-reporting of disease<br>❑ Investigations<br>❑ Interventions<br>❑ Foreign governments collaborating w/US public health authorities<br>**Communicable disease (also report to ambulette/EMS transporter)** | Facility may disclose protected health information for public health activities and purposes to:<br>1) A public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority; or<br>2) A person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if the Facility or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation. |
| **Research** | Yes, must be approved by FAS Legal Department |

| Disclosures to or for: | Is a HIPAA Authorization Required? |
|---|---|
| **Reporting Abuse, Neglect or Domestic Violence** | Except for reports of child abuse or neglect permitted as a disclosure to a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect, the Facility may disclose protected health information about an individual whom the Facility reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:<br>1) To the extent the disclosure is required by law and the disclosure complies with and is limited to the relevant requirements of such law;<br>2) If the individual agrees to the disclosure; or<br>3) To the extent the disclosure is expressly authorized by statute or regulation and:<br>A) In the exercise of professional judgment, the Facility believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or<br>B) If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the protected health information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure. |
| | i. Informing the individual. If the Facility makes a disclosure about victims of abuse, neglect or domestic violence in accordance with this section, the Facility must promptly inform the individual that such a report has been or will be made, except if:<br>a.) In the exercise of professional judgment, the Facility believes informing the individual would place the individual at risk of serious harm; or<br>b.) The Facility would be informing a legal representative, and the Facility believes the legal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as the Facility determines in the exercise of professional judgment. |
| **State Surveyors**<br>❑ Annual Surveys<br>❑ Complaint Surveys | No |
| **Secretary of Health & Human Services**<br>❑ Determining compliance with the HIPAA Privacy Rules | No |

| | |
|---|---|
| **Social Security Administration**<br>❑ Disability verification | Yes |
| **Workers Compensation**<br>❑ Comply w/existing laws (see state law) | Facility may disclose protected health information as authorized by and to the extent 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 without regard to fault. |

***MEDICAL RECORDS REQUEST***
***FAX COVER SHEET***

Date: _____

To: _____ Fax No.: 410-773-1029

From: _____ Phone No. _____

Health Care Center: _____ Fax No. _____

City & State: _____ Alternate Contact: _____

This health care center has received the following request for release of medical records:

□ Subpoena (only answer #5 below) □ Letter requesting records

Patient/Resident: _____ Admitted From: _____ to _____

*INSERT ADMIT/DISCHARGE DATES*

Please review and advise regarding the release of these records. I have examined this request thoroughly AND have noted the following **(Check ONLY those that apply)**:

| | | Yes | No |
|---|---|---|---|
| 1. | The patient/resident signed this authorization | | |
| | AND his/her signature matches our Admissions paperwork or his/her signature has been witnessed/notarized on the request. | | |
| 2. | The patient/resident is capable of making his/her own health care decisions. | | |
| | If the patient/resident is not capable, has the physician provided written certification? | | |
| 3. | The person signing this authorization is the patient's/resident's Healthcare Power of Attorney or Guardian.<br>**A copy of this documentation is attached for your review.** | | |
| 4. | The patient/resident is deceased | | |
| | AND the person signing the authorization has been named by the Probate Court as the Executor/Administrator Estate, OR, there is no Estate and the person signing the authorization has been named in the Last Will and Testament as the Personal Representative. (If neither is true, call FAS Legal for further guidance.)<br>A copy of this documentation is attached for your review. | | |
| 5. | The following incident reports are on record for this patient/resident. (Please list only the dates of each occurrence and a short description. For example, "11/1 - fall with fracture".) | | |
| | | | |
| | | | |
| | | | |
| 6. | After reviewing the patient's/resident's record, if there are any concerns regarding the patient's/resident's care noted, please have the Administrator or DON contact the FAS Legal Department to discuss. | | |

**Exhibit B**

CHECKLIST

**Worksheet for preparing a record for release when photocopies are made.**
**Do Not Include with the Released Medical Record.**

Patient Name: Date of Birth: _____

- ☐ Verify that each page (front and back) of the medical record contains the patient/resident name and medical record number (MRN).
- ☐ If the entire medical record is requested, number each page (front and back) prior to copying.
- ☐ If only a portion of the medical record is requested, only those specific pages are photocopied. These photocopies are numbered or identified is some fashion so that if submitted to a Court or Administrative Organization for review, missing pages are apparent.
- ☐ Draw a large "X" through any blank areas within the record, blank pages or the back of pages used for documentation purposes (i.e., ***Interdisciplinary Progress Notes, Physician progress notes, etc***). A single line may be drawn through blank areas that are only a few lines.
- ☐ Reduce the photocopy to 92% of the original size. *(Verifies that any documentation in the margin of the record is included on each copy*.)
- ☐ Copy the front and back of each document. *(This is done to show that the entire record has been copied and released.)*
- ☐ Carefully, review photocopies for legibility. Documents on colored paper may have poor copy quality. Colored documents may need manual "Light….Dark" adjustments on the copy machine.
- ☐ If the Physician's Telephone Orders or Lab Reports are "shingled", copy them individually so every order is legible.
- ☐ Place chart dividers (use paper dividers) in every copy of the record prepared for delivery/release.
- ☐ Place a photocopy of the record in a three-ring binder, manila folder or an envelope. If a folder is used, use a rubber band or other fastener to secure the pages together. Do not have any loose pages!
- ☐ Organize the photocopy of the record in the same manner as the original or stored record.
- ☐ Include the Confidentiality Statement as the top sheet.
- ☐ Complete a final review of the record to be released to verify that the record is prepared appropriately.

Signature: _____ Date: _____ ---_____

IMPORTANT NOTE:

FIRST IMPRESSIONS MAKE A LASTING IMPRESSION. THEREFORE, IT IS IMPORTANT TO PREPARE A NEAT, LEGIBILE AND EASY TO HANDLE DOCUMENT/RECORD FOR REVIEW.

Note: This form is **NOT** a part of the medical record. It is to be used as a worksheet only. The checklist may be destroyed after use. However it may be useful to retain the checklist for thirty (30) days.

## Exhibit C: Confidentiality Statement

* * * * * * * * * * * * * * * * * *

**THIS INFORMATION IS**

**CONFIDENTIAL AND**

**IS PROTECTED BY**

**FEDERAL AND STATE STATUTES.**

* * * * * * * * * * * * * * * * * *

**SUBJECT: MINIMUM NECESSARY USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION**

**POLICY:**

The Facility makes reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request, unless an exception applies. The Facility identifies persons or classes of persons in its workforce who need access to PHI to carry out their duties and the category or categories of PHI to which access is needed and any conditions appropriate to such access.

**The Facility may not use, disclose or request an entire Medical Record, except when the entire Medical Record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request.**

**PROCEDURES:**

**1. General Rule:** When using or disclosing PHI, or when requesting PHI from another covered entity, the Facility makes reasonable efforts to limit the PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. This General Rule does not apply to the following:

A. Disclosures to, or requests made by health care providers who are involved in the patient's/resident's care for treatment purposes.
B. Uses or permitted disclosures to the patient/resident.
C. Uses or disclosures made pursuant to an authorization.
D. Disclosures made to the Secretary of the U. S. Department of Health and Human Services.
E. Uses or disclosures that are required for compliance with the HIPAA Privacy Rule or other laws.

2. The Facility has identified the following classes of persons in its workforce with respect to access to PHI for patients/residents who are under their care or responsibility:

A. Level One. Individuals designated in this category have no access to PHI.
B. Level Two**.** Individuals in this category may access minimum necessary PHI (not the Designated Record Set) to complete assigned tasks and/or to document actions.
C. Level Three**.** Individuals in this category have full access to the Medical Record subset of the Designated Record Set.
D. Level Four. Individuals in this category have full access to the Business Office File subset of the Designated Record Set.
E. Following this policy is *Exhibit A: "Role-Based Access to PHI*" that identifies the job categories in the Facility and designates the level of access. **Facilities may modify this table to include additional job categories and to designate the appropriate level of access.**

3. Health care providers who are not part of the Facility's workforce but are involved in the patient's/resident's care, have access to the patient's/resident's medical record for treatment purposes only.

**SUBJECT: MINIMUM NECESSARY USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION (Continued)**

4. The Facility Privacy Officer may grant permission for other persons or classes of persons or entities to access a patient's/resident's Medical Record for the purposes of treatment.

5. The Facility Privacy Officer may grant permission for other persons or classes of persons or entities to access a patient's/resident's Business Office File for the purposes of payment or health care operations.

6. Disclosures of PHI that occur on a routine and recurring basis, and to which the minimum necessary policy applies, are limited to the amount of PHI reasonably necessary to achieve the purpose for the disclosure.

Examples of Routine and Recurring Disclosures

| **Requestor** | **Purpose of Disclosure** | **PHI Disclosed** |
|---|---|---|
| Ambulance Company | Obtain demographic and insurance information for billing | Face sheet containing patient/resident demographics, diagnoses and insurance information. |
| Collection Agency or Attorney assisting with Collections | Obtain payment on past due account. | Patient/resident name, demographic information, dates of service, amount owed, and collection activities to date. |
| Funeral Director | Obtain PHI necessary to carry out their functions. | Patient/resident demographic information, diagnoses. |
| Disability Determination | Evaluate individual's medical condition in support of disability benefits | Specific information requested |
| Employer | Evaluate utilization | Plan summary information (aggregate information not individually identifiable) |
| Insurance Co | Substantiate care provided for payment | Specific information requested in claims attachment request |
| Life Insurance | Evaluate individual's medical condition for issuance of a life insurance policy | Discharge summaries for specified period of time |
| Patient/Resident | 1. Amend patient's/resident's PHI<br>2. Per patient's/resident's request' | Information specified by patient/resident |
| Pharmacy | Obtain demographic and insurance information for billing | Face sheet with patient demographics, diagnoses and insurance information |
| Physician or other practitioner | Obtain demographic and insurance information for billing | Face sheet with patient demographics, diagnoses and insurance information |

**SUBJECT: MINIMUM NECESSARY USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION (Continued)**

**7. Other Disclosures:** For any disclosure that does not occur routinely, the Facility evaluates the disclosure to determine if the PHI to be disclosed is reasonably necessary to accomplish the purpose for which the disclosure is sought. The following criteria is used in making this evaluation:

A. Is the purpose for the disclosure stated with specificity?
B. Is the amount of PHI to be disclosed limited to the stated purpose?
C. Have the requirements for supporting documentation, statements, or representations been satisfied? See policy **Request and Reporting Disclosure Table** in the policy, **Disclosure of Protected Health Information (PHI)/Medical Records.**
D. Have all applicable requirements of the HIPAA Privacy Rule been satisfied with respect to the disclosure?

**8. Reasonable Reliance:** The Facility may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose in the following circumstances:

A. The disclosure is made to a public official who represents that the PHI requested is the minimum necessary.
B. The information is requested by another covered entity.
C. The PHI is requested by a professional who:
    1) Is a member of the Facility workforce or a Business Associate of the Facility;
    2) Is providing professional services;
    3) Is involved in the patient's/resident's care; and
    4) Represents that the PHI requested is the minimum necessary for a stated purpose.
    5) For research purposes, if the documentation or representation requirements of the HIPAA Privacy Rule have been met.
D. Contact the Fundamental Administrative Services, LLC Privacy Officer to assist in determining whether such requirements have been met.

**Examples of Non-Routine Requests and Disclosures**

| Requester | Purpose | Disclosures |
|---|---|---|
| Coroner | Investigate a suspicious death | Specific information requested |
| Genetic testing | DNA testing | Per response to criteria and review committee decision |
| Law enforcement | To locate a fugitive, missing person, material witness or suspect of a crime | Per response to criteria and review committee decisions: *may include:*<br>• Name and address<br>• Date and place of birth<br>• Social security #<br>• ABO blood type<br>• Type of injury<br>• Date and time of treatment<br>• Date and time of death<br>• Description of physical characteristics<br><br>**DO NOT DISCLOSE ANY DNA analysis, dental records or typing, sample of analysis of body fluids** |
| National Security | Varies | Specific information requested by agencies (CIA, FBI, etc.) |
| Organ/tissue donations | Qualify donation use (academic, transplant etc.) | Per response to criteria and review committee decision |
| Public Official | Investigate accidents or crimes | Specific information requested |
| Healthcare oversight agency | Investigate a complaint | Protected health information related to complaint |
| State data commission | Support a state wide registry | File of specific data elements requested |
| Researcher | Treating a patient/resident in a clinical trial | Full access to medical record for treatment purposes |

**9. Facility Requests for PHI from Another Health Care Provider:** When requesting PHI from another health care provider, the Facility limits its request for PHI to the amount reasonably necessary to accomplish the purpose for which the request is made.

A. For requests that are made on a routine and recurring basis, the Facility takes reasonable steps to limit the request to the amount of PHI reasonably necessary to accomplish the purpose for which the request is made.

B. For requests that are not on a routine or recurring basis, the Facility evaluates the request according to the following criteria:

1) Is the purpose for the request stated with specificity?

2) Is the amount of PHI to be requested limited to the intended purpose?

**SUBJECT:** **MINIMUM NECESSARY USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION (Continued)**

3) If applicable, is there HIPAA compliant Authorization signed by the Patient/Resident or the Legal Representative. See policy on **Authorization to Disclose/Release Information** form.
4) Have all applicable requirements of the HIPAA Privacy Rule been satisfied with respect to the request?

**REFERENCES:**

1. **HIPAA Final Privacy Regulations**
45 CFR § 164.514(d)(1)

## Exhibit A: Role Based Access to PHI

***LEVEL 1:*** *None – No Access to Designated Record Set (Ex: Volunteer)*
***LEVEL 2:*** *May access minimum necessary PHI (not Designated Record Set) to complete assigned tasks and/or to document actions (Ex: PHI discussed)*
***LEVEL 3:*** *Full access to the Medical Record subset of the Designated Record Set*
***LEVEL 4:*** *Full access to the Business Office File subset of the Designated Record Set*

| **Position** | **Access Level** | | | | **Explanation/Duties Performed Requiring Access** |
|---|---|---|---|---|---|
| | **1** | **2** | **3** | **4** | |
| Administrator/Executive Director | | | X | X | |
| Admissions | | X | | | |
| Billing Office Staff | | | | X | |
| Nurse | | | X | | |
| Nurse Manager | | | X | | |
| Receptionist | | X | | | |
| Therapist | | | X | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

**SUBJECT: DISCLOSURE OF PROTECTED HEALTH INFORMATION TO INDIVIDUALS INVOLVED IN THE PATIENT'S/RESIDENT'S CARE**

**POLICY:**

Upon written authorization from the patient/resident or his/her legal representative, facility staff discloses protected health information (PHI) to other individuals involved in the patient's/resident's care for the sole purpose of keeping those individuals informed of the patient's/resident's condition, progress, treatment, and care while at the facility. Prior to disclosing information to individuals other than the patient/resident, facility staff determines if those individuals are authorized to receive information and requests identification to confirm their identity.

Due to the risks and consequences involved in the disclosure of PHI, the facility's policies prohibit the disclosure of information to individuals other then the patient/resident or his/her legal representative and we do not recommend bypassing these policies. However, there may be situations where an exception to these policies needs to be made and a patient/resident or the legal representative specifically requests that our staff communicate with other individuals regarding the patient's/resident's treatment and care. This policy and form are to be used on a case-by-case basis, as the need arises.

*This policy and form do NOT authorize any individual to make health care decisions on behalf of the patient/resident. In addition, this policy and form do NOT authorize the release of medical records; see "Disclosure of Protected Health Information (PHI)/Medical Records" policy.

**This policy and form are NOT part of the admission process as they are provided only as an exception to the facility's policy that information is not provided to any individuals other than the patient/resident or the legal representative.

**PROCEDURES:**

1. The Privacy Designee or his/her designee manages requests for disclosure of PHI to individuals involved in the patient's/resident's care.

2. When the patient/resident or legal representative requests that PHI be disclosed to individuals involved in the patient's/resident's care, the Privacy Designee or his/her designee provides the patient/resident or legal representative with the **Authorization & Consent for the Release of Protected Health Information (PHI) to Individuals Involved in the Patient's/Resident's Care** form (FFIP032P) available on the Fundamental Resource Center for completion.

3. It is essential that the individual signing this form, if other than the patient/resident, is legally authorized to act on the patient's/resident's behalf. Each state has different requirements defining an authorized representative. Therefore, we recommend that you contact the Fundament Administrative Services, LLC Legal Department if assistance is needed in determining an individual's authority to act on behalf of the patient/resident.

4. If the patient/resident or legal representative wishes to restrict the information to be disclosed under #2 of the form, refer to the **Restriction of Protected Health Information** policy in this manual.

**SUBJECT:** **DISCLOSURE OF PROTECTED HEALTH INFORMATION TO INDIVIDUALS INVOLVED IN THE PATIENT'S/RESIDENT'S CARE (Continued)**

5. Once a completed form is received, notify the individuals identified on the authorization, under separate cover, of the personal identification number (PIN) assigned for the patient/resident. The PIN (such as the last 4 digits of the patient's/resident's social security number or the patient's/resident's medical record number) is determined by the Facility.

6. Provide a copy of the completed **Authorization & Consent for the Disclosure of Protected Health Information (PHI) to Individuals Involved in the Patient's/Resident's Care** form to the patient/resident or the legal representative.

7. Document the PIN on the **Authorization & Consent for the Disclosure of Protected Health Information (PHI) to Individuals Involved in the Patient's/Resident's Care** form and file the form under the **HIPAA tab** in the patient's/resident's medical record.

8. Prior to disclosing information to an individual other than the patient/resident, Facility staff refers to the **Authorization & Consent for the Disclosure of Protected Health Information (PHI) to Individuals Involved in the Patient's/Resident's Care** form in the medical record to determine that the individual is authorized to receive the information.

9. Facility staff confirms the individual's identity either in person by requesting identification, such as a driver's license, or over the phone by requesting the assigned PIN.

**SUBJECT: PATIENT'S/RESIDENT'S ACCESS TO PROTECTED HEALTH INFORMATION/MEDICAL RECORD**

**POLICY:**
Each patient/resident has the right to access his/her own Protected Health Information (PHI) as specified in the Notice of Privacy Practices. Some states may have more stringent regulations regarding patient/resident access to his/her medical/financial records. If a State has a more stringent requirement, the Facility must comply with the State law.

**DEFINITIONS:**

**Protected Health Information (PHI):** Is defined as individually identifiable health information that is maintained or transmitted by a healthcare provider in any form, including electronic records, paper records and oral discussions. Some examples of protected health information are interdisciplinary progress notes, physician's orders, care plans and billing information that contains patient/resident health information.

**Designated Record Set (DRS):**
A group of records maintained by the facility that consists of the medical records and billing records for the patient/resident and that is used by the facility to make decisions about the patient/resident. The designated record set includes billing information that may contain ICD-9-CM codes that represent conditions of the patient/resident and are protected health information.

For access to the Designated Record Set, The State Operations Manual (F153) allows the patient/resident to "have access to all records pertaining to himself or herself including current clinical records." The Guidance to Surveyors indicates that the term "records" includes "all records pertaining to the patient/resident such as trust fund ledgers pertinent to the patient/resident and contracts between the patient/resident and the facility."

The SOM (F164) further defines personal records in the Guidance to Surveyors to include all types of records the facility might keep on a patient/resident, whether they are medical, social, fund accounts, automated or other.

**Legal Representative:** If the patient/resident is a minor, is incompetent or deceased, the release form is signed by his/her legal representative.

A. In the case of a minor this would include a parent, probate conservator, guardian or any other person who has lawful custody.

B. In the case of incompetent adult patients/residents:

1) a probate guardian/conservator of the patient's/resident's person or psychiatric guardian/conservator of the patient's/resident's person;
2) a Power of Attorney designated in writing by the patient/resident; or
3) a Health Care Surrogate under applicable state law.

C. In the case of a deceased patient/resident this would be the person who has been declared the executor or the administrator of the patient's/resident's estate. Court documentation regarding the identity of the executor must be received prior to release.

A "responsible party" is **not** the patient's/resident's "legal representative" **unless** they are the patient's/resident's Health Care Power of Attorney, Guardian, Parent of a Minor, or Health Care

Surrogate under applicable state law.
For questions regarding a person's authority to act on behalf of a patient/resident, contact the Fundamental Administrative Services, LLC Legal Department.

**PROCEDURES:**

1. A patient/resident or his/her legal representative has the right to access, inspect and request copies of his/her own Designated Record Set unless State Law allows for restrictions. The Facility may deny a patient/resident access if a licensed health care professional has determined, in the exercise of professional judgment, that:
   A. The access requested is reasonably likely to endanger the life or physical safety of the individual or another person.
   B. The access requested makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person.
   C. The request for access is made by the patient's/resident's legal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

If access is denied as specified above, see #5 below, Denial of Access

2. The Privacy Designee or his/her designee manages all requests for patient/resident access to PHI.

3. **Requests for Copies of the Medical Record**
   A. The facility provides copies within 48 hours (excluding weekends and/or holidays) unless State law mandates a shorter period. If State Law mandates a shorter period for responding, then you are obligated to meet the State's more stringent requirement.
   B. Upon receiving a request from a patient/resident to receive a copy of his/her PHI, Privacy Designee or his/her designee may provide a copy of the **Authorization & Request for Release of Information (NFF-IP020P)** on the Fundamental Resource Center (FRC) for completion and execution**. HIM Staff may also accept any written request that is signed by the patient/resident or legal representative if the records are being released directly to the patient/resident or legal representative.**
   C. Review the Authorization for accuracy and completeness against the Authorization Checklist below.
   D. **If any of the steps above are incomplete**, ask the patient/resident or the legal representative to fill in the missing information.
   E. If the patient/resident or legal representative is requesting electronic copies of their PHI, see #7 **Providing Electronic Copies** below.
   F. Once it is determined that the Authorization is complete:
      1) Document the request on the **HIPAA Correspondence Log** in The HIM Department. (See **HIPAA Documentation** policy.)
      2) Continue with Step 2 of policy **Disclosure of Protected Health Information (PHI)/Medical Records.**

**SUBJECT: PATIENT'S/RESIDENT'S ACCESS TO PROTECTED HEALTH INFORMATION/MEDICAL RECORD (Continued)**

4. **Providing Access to view/review PHI**
   - A. If a patient/resident requests, either orally or in writing, access to view his/her medical/financial record, an appointment is coordinated with the Privacy Designee or his/her designee to oversee the review.
   - B. The appointment is scheduled within twenty-four (24) hours of the request pursuant to Federal regulations or if State law mandates a different time period then you are obligated to meet the State's requirement.
   - C. If the patient/resident requests copies after reviewing the medical record, follow the procedures starting with 3B above and obtain a signed authorization from the patient/resident.
   - D. The facility provides the patient/resident with access to the PHI in the form or format requested. If the PHI is not accessible in the format requested, a readable hard copy or a format to which the facility and the patient/resident agree is acceptable.

5. **Denial of Access**
   - A. The Facility makes reasonable efforts to provide access to all records that do not provide grounds for denial.
   - B. In all cases in which access to records is denied, the patient/resident is notified in writing of a decision to deny access to all or part of the designated record set, including a short statement of the basis for the denial.
   - C. The notice contains the following:
     1) Information on how the patient/resident may contact the Administrator,
     2) How to file a complaint with the Department of Health and Human Services, and
     3) How the patient/resident may file an appeal with the Facility.
   - D. The Denial of Access to Protected Health Information form is available on the FRC.

6. **Denial of Access Appeal**
   - A. The appeal is an internal review process to review the initial decision to deny access to a record and determine whether that denial satisfied the grounds for denial.
     1) All appeals must be submitted in writing.
     2) Upon receipt of a written appeal, the Director of HIM forwards the appeal and the reasons for denial to the Medical Director.
   - B. The Privacy Designee or his/her designee will confer with the Medical Director or equivalent authority to review the matter.
   - C. The appeal review will be completed in a reasonable timeframe. The reviewer will provide a decision in writing to the Privacy Designee or his/her designee.
   - D. Upon receipt of the appeal review decision, the Privacy Designee or his/her designee will notify the patient/resident promptly in writing.
   - E. Documentation of the denial, the patient's/resident's written appeal, the appeal reviewer's decision, and the notice to the patient/resident will be maintained in the HIPAA Correspondence Log.

**SUBJECT: PATIENT'S/RESIDENT'S ACCESS TO PROTECTED HEALTH INFORMATION/MEDICAL RECORD (Continued)**

7. **Providing Electronic Copies**

A. If the Facility maintains electronic PHI, the Facility provides the patient/resident or legal representative with a copy of their PHI in the electronic form and format requested by the individual if such format is readily producible. *The Facility is not required to scan records maintained in hard copy*.

B. If the requested format is not readily producible, the Facility must offer to produce the electronic PHI in at least one readable electronic format.

1) A hard copy may be provided if the requesting patient/resident or legal representative rejects any of the offered electronic formats.

C. The electronic copy provided must include all electronic PHI held by the Facility in a designated record set, or appropriate subset if only specific information is requested, at the time the request is fulfilled.

D. If the Facility maintains medical records in mixed media (i.e., some paper and some electronic PHI), a combination of electronic and hard copies may be provided to the patient/resident or legal representative.

E. The Facility **only** uses an encrypted flash drive or other portable media provided by the Fundamental Administrative Services, LLC (FAS) IS Department to transfer the electronic PHI. Encrypted flash drives are purchased through DSSI. Non-Fundamental issued devices/media **are not** connected to the Facility network or equipment without the express approval of the FAS IS Department pursuant to the *Hardware/Software Policy*.

1) The Facility cannot require the patient/resident or legal representative to purchase a portable media device from the Facility. The patient/resident or legal representative may opt to receive an alternative form of the electronic copy of the PHI, such as through email.

F. The patient/resident or legal representative may request that the electronic PHI be sent via unencrypted email. **This is the ONLY circumstance where PHI can be sent unencrypted via email.**

1) In this circumstance, the request must be in writing and clearly identify the designated person and where to send the copy of the electronic PHI.

2) In addition, the Facility must advise the patient/resident or legal representative regarding the risks associated with sending PHI via unencrypted email.

G. The Privacy Designee or his/her designee provides the patient/resident or legal representative with the **Request for Electronic Protected Health Information** form available on the FRC for completion and execution. **No** electronic protected health information is released until the Facility receives a completed and signed form.

H. The Privacy Designee or his/her designee mails or emails the electronic protected health information to the address or email address provided on the **Request for Electronic Protected Health Information** form.

I. The Facility can only charge for the costs of supplies for creating electronic media (e.g., flash drives) if the patient/resident or legal representative requests the copy on portable media and for postage if the patient/resident or legal representative requests mailing or delivery of electronic media. This is in addition to any fees allowed by state law for providing hard copies of records if hard copies are also provided in response to the request.

**SUBJECT: PATIENT'S/RESIDENT'S ACCESS TO PROTECTED HEALTH INFORMATION/MEDICAL RECORD (Continued)**

**REFERENCES:**

1. **HIPAA Final Privacy Regulations**
   45 CFR § 164.524
   45 CFR § 164.520

## Authorization Checklist

1. Review of the Authorization & Request for Release of Information
   - ❑ Does the authorization specifically identify the patient/resident?
   - ❑ Is the authorization specifically addressed to the facility or the Administrator in the facility?
   - ❑ Does it identify the individual or entity authorized to receive the information?
   - ❑ Is the information authorized for disclosure identified? (i.e. Does it specify the medical record document(s) requested and dates to be included?)
   - ❑ If all records are requested and the authorization is valid, you may copy and send all information.
   - ❑ Does the authorization address the purpose for this release? When the patient/resident initiates the authorization and elects not to provide a statement of purpose, a statement "at the request of the individual" is a sufficient description.
   - ❑ Did the patient/resident or the patient's/resident's legal representative sign and date the authorization? Refer to #2 below for guidance.
   - ❑ If the signature is someone other than the patient/resident, is there an explanation of that person's relationship to the patient/resident? (For example, DPOA, Executor, etc.)
   - ❑ Is the date on the authorization after the patient's/resident's admission to the facility?

2. Who is authorized to sign the authorization for release of protected health information?
   - A. If the patient/resident has the capacity, he/she retains the right to sign the authorization.
   - B. If the patient/resident does not have the capacity, the legal representative, if one exists, can sign the authorization.
     1) If the requestor is a legal representative or guardian, he/she has the appropriate paperwork on file with our facility (Durable Power of Attorney, court order, etc.).
   - C. If no legal representative, seek guidance from your state contact in the FAS Legal Department.
   - D. If the patient/resident is deceased, it is generally the executor of the estate or it may be the next of kin. State law is researched to determine who has this authority for a deceased patient/resident. If in doubt, consult your state contact in the FAS Legal Department.

**SUBJECT:** **BREACHES OF PROTECTED HEALTH INFORMATION**

**POLICY:**
The Facility provides notification to affected patients/residents of breaches of their Protected Health Information ("PHI").

**A. Definitions**

1. Breach – the term "breach" means the unauthorized acquisition, access, use, or disclosure of Unsecured PHI which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.
   A. For purposes of this definition, "compromises the security or privacy of PHI" means the breach poses a significant risk of financial, reputational, or other harm to the patient/resident.
   B. The term "breach" does not include any unintentional acquisition, access, or use of PHI by an employee or person acting under the authority of the Facility or a Business Associate if:
      1) Such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship between the employee or person and the Facility or a Business Associate; and
      2) Such information is not further acquired, accessed, used, or disclosed in a manner that would violate the Privacy Rule; or
      3) Any inadvertent disclosure from an individual who is otherwise authorized to access PHI at the Facility or the Business Associate to another person authorized to access PHI at the Facility or at the same Business Associate; and
      4) Any such information received as a result of such disclosure is not further used or disclosed in a manner that would violate the Privacy Rule.
         a) For an acquisition, access, use or disclosure of PHI to constitute a breach, it must constitute a violation of the Privacy Rule. *A use or disclosure of PHI that is incidental to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule and would not qualify as a potential breach.*
2. Unsecured PHI – PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary of Health and Human Services.

**B. Breach Investigation**

1. The Facility and its employees report potential breaches to the InTouch Hotline at 800-255-4730.
2. Following discovery of a potential breach, the Facility conducts an investigation with the assistance of the Fundamental Administrative Services, LLC (FAS) Legal Department and Privacy Officer which includes a risk assessment to determine if a breach has occurred.

**SUBJECT:** **BREACHES OF PROTECTED HEALTH INFORMATION (Continued)**

**C. Discovery of Breach**

1. In the event the Facility determines that a breach of Unsecured PHI occurred, the Facility notifies each affected patient/resident.
2. The notification requirement applies to any breach of Unsecured PHI maintained by the Facility or its Business Associates.
3. For purposes of this Procedure, a breach is treated as "discovered" by the Facility as of the first day on which the breach is known to the Facility (including any person, other than the person committing the breach, that is an employee, officer, or other agent of the Facility), or by exercising reasonable diligence would have been known to the Facility. The breach is also "discovered" when the Facility is informed by one of its non-agent Business Associates, (including any person, other than the person committing the breach, that is an employee, officer, or other agent of the Business Associate), or by exercising reasonable diligence would have been known to the Business Associate to have occurred.

**D. Timeliness of Notification**

1. Unless otherwise specified below, Facility provides notifications of a breach of Unsecured PHI as soon as practicable and in no case later than sixty (60) calendar days after the discovery of a breach.
2. Notification may be delayed if a law enforcement official determines that a notification, notice or posting would impede a criminal investigation or cause damage to national security. If a verbal request to delay notification is received, the Facility shall delay the notification up to thirty (30) days. If the law enforcement official requests a delay in notification in writing with a specified time for delay, the Facility shall honor the time delay as specified.

**E. Methods of Notice**

**1. Patient/Resident Notice** – Notice of a breach provided to an patient/resident must meet the following requirements:

A. The notice must be written in plain language and delivered to the patient/resident by first-class mail addressed to the patient/resident (or the next of kin of the patient/resident if the patient/resident is deceased) at the patient's/resident's (or next of kin's) last known address. In the alternative, if the patient/resident (or next of kin) has so specified, the notification may be delivered by electronic mail. The notification may be provided in one or more mailings as information becomes available.

B. In the case in which there is insufficient, or out-of-date contact information (including a phone number, email address, or any other form of appropriate communication) that precludes direct written (or, if specified by the patient/resident, electronic) notification, a substitute form of notice must be provided.

1) Where there is insufficient or out-of-date contact information for less then 10 patients/residents, a substitute notice may be provided by an alternative form of written notice, by telephone, or by other means.

**SUBJECT:** **BREACHES OF PROTECTED HEALTH INFORMATION (Continued)**

2) Where there are ten (10) or more patients/residents for which there is insufficient or out-of-date contact information, a conspicuous posting for a period of ninety (90) days on the home page of the website of the Facility or notice in major print or broadcast media, including major media in geographic areas where the patients/residents affected by the breach are likely reside. Such a notice in media or a web posting will include a toll-free number where an patient/resident can learn whether or not the patient's/resident's Unsecured PHI is possibly included in the breach.

3) Where there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of a deceased patient/resident, a substitute notice is not required.

a) If the Facility determines that immediate notification is required because of possible imminent misuse of Unsecured PHI, the Facility may provide information by telephone or other means, as appropriate, in addition to the written notification required.

**2.** **Media Notice** – Notice shall be provided to prominent media outlets serving the State or jurisdiction following the discovery of a breach of Unsecured PHI if the Unsecured PHI of more than 500 patients/residents is, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach.

**3.** **Notice to Secretary** – Notice is provided to the Secretary of Unsecured PHI that has been acquired or disclosed in a breach. For a distinct breach involving 500 or more patients/residents, the Facility must notify the Secretary of HHS immediately. For a distinct breach of less than 500 patients/residents, the Facility may maintain a log of any such breach occurring and annually submit the log to the Secretary documenting the breaches occurring during the year involved.

**F. Content of Notification**

1. Regardless of the method by which notice is provided to patients/residents as set forth above, notice of a breach is in plain language and includes, to the extent possible, the following:
   a) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
   b) A description of the types of Unsecured PHI that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).
   c) The steps patients/residents should take to protect themselves from potential harm resulting from the breach.
   d) A brief description of what the Facility is doing to investigate the breach, to mitigate harm to the patients/residents, and to protect against any further breaches.
2. The notification must also include contact procedures for patients/residents to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or postal address.

**SUBJECT:** **BREACHES OF PROTECTED HEALTH INFORMATION (Continued)**

**G. Documentation**

1. The Facility documents its investigation and provision of the notification to affected patients/residents where applicable.
2. All documentation related to the breach investigation and provision of the notification is retained for a minimum of six years.

**REFERENCE:**

1. **HIPAA Breach Notification Rule**
   45 CFR § 164.400

## SUBJECT: BUSINESS ASSOCIATE POLICY

### POLICY:

The Facility contracts with various outside entities and organizations to perform functions or provide services on behalf of the Facility that may involve the disclosure of Protected Health Information ("PHI") to the outside entity. These outside entities are the Facility's Business Associates (BA). The Facility obtains written assurances from its BAs that they will appropriately safeguard any PHI they create or receive on the Facility's behalf. Such written assurances are in place before the Facility discloses PHI to the Business Associate.

### PROCEDURES:

1. The Facility Administrator forwards contracts to the Fundamental Administrative Services, LLC (FAS) Legal Department for review.

2. The contract is reviewed to determine whether a Business Associate Agreement is necessary. (See the attached *Business Associate Decision Tree.*) Common examples of BAs are:
   A. The Facility's Medical Director
   B. The Facility's pharmacy consultant that conducts MAR reviews to assist the Facility with regulatory compliance
   C. An attorney who reviews patient/resident information to assist in the appeal of a survey citation or any other matter that requires the disclosure of PHI to the attorney
   D. A Medical Records Consultant
   E. A Record Storage Company

   ***Note*:** Business Associate language is ***not*** required when the BA is a health care provider and all disclosures to the BA concern the treatment of a patient/resident.

3. If a BA Agreement is necessary and the third party provides its own BA Agreement, forward the BA Agreement to the FAS Legal Department for review.

4. If a BA Agreement is necessary and the third party does not provide the Agreement, the Facility's BA Agreement is submitted to the third party for approval.

5. If the BA refuses to sign the BA Agreement, the HIPAA Privacy Rule prohibits the Facility from disclosing any PHI to the BA. If the BA requires access to PHI in order to perform the function or service on behalf of the Facility, the Facility does not contract with the BA. Contact the FAS Legal Department for further assistance.

6. The original signed contract and contract addendum containing BA language is maintained by the Facility.

7. Violations of BA Requirements - If Facility staff learn of a breach or violation of a BA requirement by a BA, such breach or violation is reported to the FAS Privacy Officer. The FAS Privacy Officer will assist the Facility in determining whether reasonable steps can be taken to cure the breach. If the Facility's reasonable steps to cure the BA's violations are unsuccessful, the Facility may:

**SUBJECT: BUSINESS ASSOCIATE POLICY (Continued)**

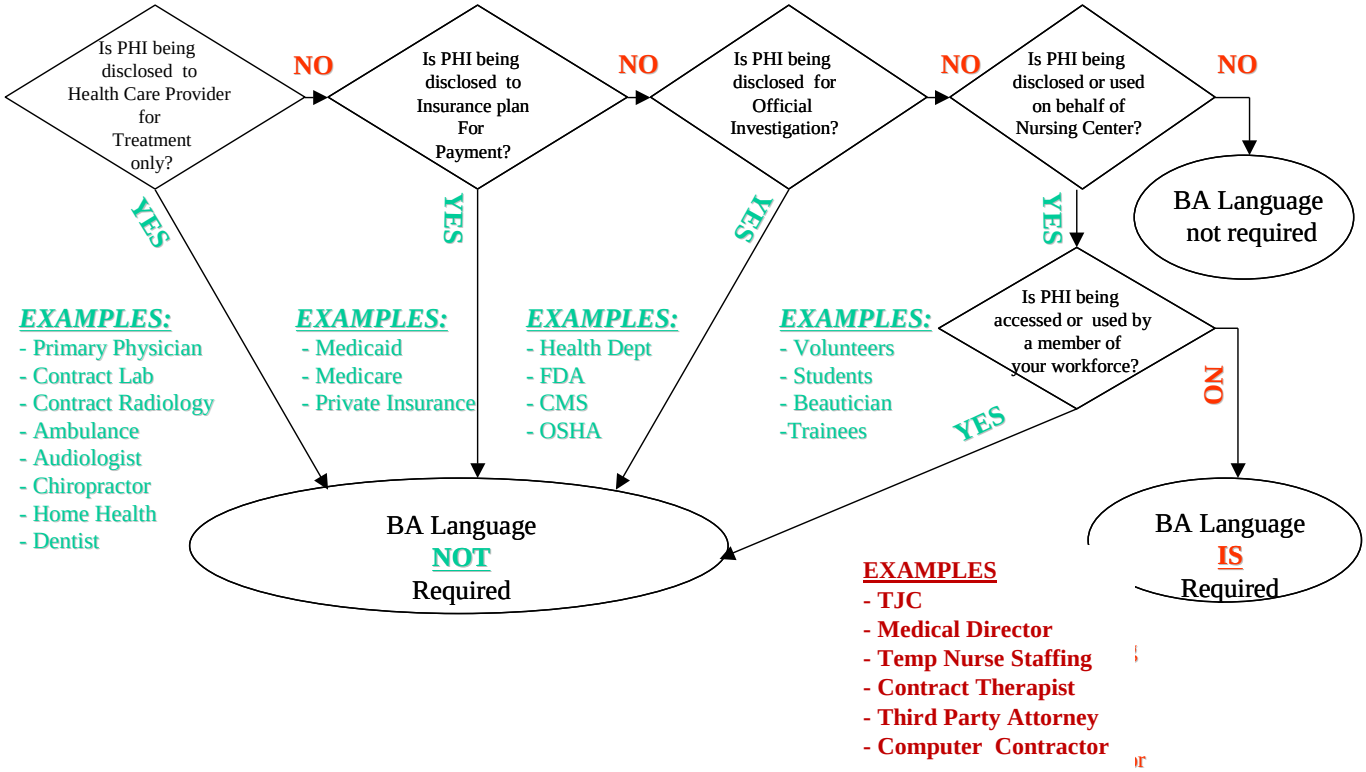
A. Terminate the contract or arrangement; or
B. If termination is not feasible, report the problem to the Secretary of the U. S. Department of Health and Human Services.

8. Termination of a Contract with a BA – Upon issuing or receiving a notice of contract termination involving a BA the Facility contacts the BA regarding the BA's obligations to return or destroy all PHI or, if return or destruction is not feasible, to extend the protections of the BA requirements to the PHI and to limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible.
The contract and contract addendum is retained for six (6) years after termination of the contract.

**REFERENCE:**

2. **HIPAA Final Privacy Regulations**
45 CFR § 164.504(e)

## *DECISION TREE: WHEN IS BA LANGUAGE REQUIRED?*



## SUBJECT: NOTICE OF PRIVACY PRACTICES

## POLICY:

1. The Facility disseminates a written notice to all patients/residents that addresses its policies and procedures with respect to the use and disclosure of protected health information and the facility's legal duties regarding such information (a "Notice of Privacy Practices").
2. The Notice of Privacy Practices includes all elements and statements that are required by law. In summary, the Notice informs the patients/residents about the potential uses and disclosures of the health information, as well as their rights with respect to that information, including:
   A. A description of each of the purposes for which the Facility is permitted to disclose their health information, including, for example, treatment, payment, and health care operations; and
   B. A description of when a written authorization is required before the Facility may disclose the patient's/resident's health information.
3. The Facility provides the Notice of Privacy Practices at the time of admission or when service is first provided to the patient/resident, whichever is first. In the case of an emergency treatment situation, provide the notice as soon as reasonably practicable after the emergency treatment situation.

## DEFINITIONS:

**Protected Health Information (PHI):** Is defined as individually identifiable health information that is maintained or transmitted by a healthcare provider in any form, including electronic records, paper records and oral discussions. Some examples of protected health information are interdisciplinary progress notes, physician's orders, care plans and billing information that contains patient/resident health information.

**Disclosure:** The release, transfer, provision of access to, or divulging in any other manner of health information.

**Treatment:** The provision, coordination, or management of health care and related services by the facility, including the coordination or management of health care by the facility with a third party; consultation with other health care providers relating to a patient/resident; or the referral of a patient/resident for health care between the facility and another health care provider.

**Payment:** The activities undertaken by a health care provider or payer to obtain reimbursement for the provision of health care.

**SUBJECT: NOTICE OF PRIVACY PRACTICES (Continued)**

**Health Care Operations:** Any of the following activities of the facility:

1. Conducting quality assessment and improvement activities, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; protocol development, case management and care coordination, contacting of health care providers and patients/residents with information about treatment alternatives; and related functions that do not include treatment;
2. Reviewing the competence or qualifications of health care professionals, evaluating employee and the facility performance, conducting training programs under supervision to practice or improve skills, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;
3. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
4. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the facility;
5. Business management and general administrative activities of the facility, including, but not limited to:
   - A. Customer service
   - B. Resolution of internal grievances
   - C. **Due diligence in connection with the sale or transfer of assets to a potential successor in interest**
   - D. Creating de-identified health information and marketing for which a patient's/resident's authorization is not required.

**PROCEDURES:**

1. The Facility provides the Notices of Privacy Practices (FFUS119) available on the Fundamental Resource Center at the time of admission or when service is first provided to the patient/resident, whichever is first. In the case of an emergency treatment situation, provide the notice as soon as reasonably practicable after the emergency treatment situation.

2. The Facility makes a good faith effort to obtain a signed acknowledgement from the patient/resident or the legal representative upon receipt of the Notice. The acknowledgement, Acknowledgement of Receipt of the Notice of Privacy Practices, is located on the last page of the Notice.

3. This acknowledgement is removed from the Notice and is kept in the patient's/resident's medical record with admissions information.

4. A copy of the signed acknowledgement is given to the patient/resident or the legal representative.

5. If a signed acknowledgement is not obtained, document the attempts and the reasons why an acknowledgement was not obtained in the section provided on the acknowledgement form.

**SUBJECT: NOTICE OF PRIVACY PRACTICES (Continued)**

1. The Facility also provides a copy of the written notice to patients/residents and to other persons upon request.

2. The Facility posts a copy of the Notice of Privacy Practices in a clear and prominent location such as the entrance lobby or other similar location.

3. A current version of the Notice of Privacy Practices is maintained on the public website.

4. If there is a material change in Facility's use and disclosure policies that affects the rights of patients/residents, legal duties imposed, or the privacy practices of the Facility, notify the Fundamental Administrative Services, LLC (FAS) Privacy Officer.

5. When the Notice of Privacy Practices is revised:
   A. The Facility distributes the revised notice promptly to current patients/residents.
   B. Make the revised notice available upon request and post in a clear and prominent location.

6. Note: Material changes cannot be implemented prior to the effective date of the revised notice.

7. Copies of Notices issued by the Facility will be maintained for at least 6 years from the date of creation or the date when it last was in effect, whichever is later.

8. Knowledge of a violation or potential violation of this policy is reported directly to the Administrator, the FAS Privacy Officer or to the InTouch Line.

**REFERENCES**

1. **HIPAA Final Privacy Regulations**
   45 CFR § 164.520

# HIPAA PRIVACY AND MEDICAL RECORD POLICIES & PROCEDURES

**SAMPLE**

## NOTICE OF PRIVACY PRACTICES

**THIS NOTICE DESCRIBES HOW YOUR MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.**
**PLEASE REVIEW IT CAREFULLY.**

This notice describes how this facility and its affiliates (together "the affiliated covered entity") may use and disclose your medical information. It also describes the facility's practices with other people that may participate in your care. The facility is required by law to provide you with this notice regarding our legal obligations with respect to your protected health information and to adhere to the terms of the notice currently in effect.

### HOW WE MAY USE AND DISCLOSE MEDICAL INFORMATION ABOUT YOU

Each time you receive treatment at the facility, a record of your treatment is made. Typically, this record contains information about your condition and the services that we provide. The following categories describe the ways that we may use and disclose your medical information. (Not every use or disclosure in a category will be listed. However, the ways we are permitted to use and disclose information typically fall into one of the categories. Also, in some cases state law limits us from disclosing specific types of health information. For example, state law usually requires that the facility get your permission before disclosing mental health, alcohol/drug use and abuse, and HIV/AIDS information.)



- **For Treatment**. We may use your medical information to treat you. We may disclose your medical information to doctors, nurses, therapists or facility personnel who are involved in taking care of you at the facility. For example, a doctor treating you for a broken leg may need to know if you have diabetes because diabetes may slow the healing process. Also, the doctor may need to tell the dietitian if you have diabetes so that we can plan your meals. Other treatment uses or disclosures of your information include sharing your medical information to provide you with medication, lab work, x-rays and other healthcare services.
- **For Payment**. We keep track of the treatment, services and supplies you receive at the facility so we can bill you, your insurance company or other third-party payer. For example, in order to be paid, we may need to share information with your health plan about services that the facility provided to you. We may also tell your health plan about a treatment you are going to receive in order to obtain pre-approval or to determine whether your plan will cover the treatment.
- **For Health Care Operations**. We use and disclose your medical information for health care operations. For example, we may use your medical information to review the treatment/services provided to you and evaluate the performance of the doctors and staff that treat you. This helps to improve our services to be sure we are providing good care. We may also combine medical information about many facility patients/residents to decide what additional services to should offer, what services are not needed, and whether certain new treatments are effective.

**OTHER USES OR DISCLOSURES OF YOUR MEDICAL INFORMATION**

- **Business Associates**. The facility provides some services by using outside vendors (also called business associates). The facility may share your medical information with them so that they can perform the job we have asked them to do including bill you or your third-party payer for services rendered. To protect your health information, however, we require the business associate to appropriately safeguard your information.
- **Treatment Alternatives**. We may use and disclose your medical information in order to tell you about possible treatment options or alternatives that may be of interest to you.
- **Health-Related Benefits and Services**. We may use and disclose your medical information in order to tell you about health-related benefits or services that may be of interest to you.
- **Facility Directory**. With your consent, we may use or disclose your information in the facility's directory.
- **Individuals Involved in Your Care or Payment for Your Care**. With your consent, we may disclose your medical information to a friend or family member who is involved in your care or for payment for your care. In addition, we may disclose your medical information to an entity assisting in a disaster relief effort so that your family can be notified about your condition, status and location.
- **As Required By Law**. We will disclose your medical information when required to do so by federal, state or local law.
- **Public Health Activities**. We may use and disclose your medical information to assist in public health activities like tracking diseases or medical devices.
- **Abuse**. We may disclose your medical information to state or federal authorities so that they can protect victims of abuse, neglect or domestic violence.
- **Health Oversight Activities**. We may disclose your medical information to a health oversight agency for activities authorized by law such as audits, investigations, and inspections.
- **Lawsuits and Disputes**. If you are involved in a lawsuit or a dispute, we may disclose your medical information in response to a court or administrative order. We may also disclose your medical information in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell you about the request or to obtain an order protecting the information requested.
- **Law Enforcement**. We may disclose your medical information to a law enforcement official.
- **Coroners, Medical Examiners and Funeral Directors**. We may disclose your medical information to a coroner/medical examiner or to funeral directors.
- **Organ and Tissue Donation**. If you are an organ donor, we may disclose your medical information to organizations that handle organ procurement in order to facilitate donation and transplantation.
- **Research**. Under certain circumstances, we may use and disclose your medical information for research purposes.
- **To Avert a Serious Threat to Health or Safety**. We may use and disclose your medical information to prevent a serious threat to your health and safety or the health and safety of the public or another person.

- **Military and Veterans**. If you are a member of the armed forces, we may disclose your medical information as required by military authorities. We may also disclose medical information about foreign military personnel to the appropriate foreign military authority.
- **National Security and Intelligence Activities**. We may disclose your medical information to authorized federal officials for intelligence, counterintelligence and other national security activities authorized by law.
- **Inmates**. We may use or disclose your medical information to inform a correctional institution if you are an inmate.
- **Workers' Compensation**. We may disclose your medical information for workers' compensation or similar programs.
- **All Other Uses** Uses and disclosures of your medical information not covered by this notice may be made only with your written authorization. You may revoke that authorization, in writing, at any time; however we are unable to take back any disclosures we have already made with your permission, and that we are required to retain our records of the care that we provided to you.
- **State Law** In some cases we are limited by state law from releasing certain categories of your medical information., such as mental health, alcohol/drug use and abuse, and HIV/AIDS information.

## YOUR RIGHTS REGARDING YOUR MEDICAL INFORMATION

Although your health record is the property of the facility, the information belongs to you. Federal law gives you the rights described below regarding your medical information.



- **Right to Inspect and Copy**. With some exceptions, you may review and copy your medical information. *****
- **Right to Amend**. You may ask us to amend your medical information if you feel it is incorrect or incomplete. However, we may deny your request under certain circumstances. *****
- **Right to an Accounting of Disclosures**. You may request an "accounting of disclosures." This is a list of certain disclosures we made of your medical information, other than those made for purposes such as treatment, payment, or health care operations. Your request must be for a period not to exceed six (6) years from the request date and may not include dates before April 14, 2003. *****
- **Right to Request Restrictions**. You may request a reasonable restriction on the uses or disclosures of your medical information. However, we are not required to agree to your request. *****
- **Right to Request Alternate Communications**. You may request that we communicate with you about medical matters in a confidential manner or at a specific location. For example, you may ask that we only contact you via mail to a post office box. *
- **Right to a Paper Copy of This Notice**. You may request a copy of this notice at any time. To obtain a paper copy of this notice, contact the facility's Administrator. You may obtain an electronic copy of this notice at our website.

* ***To exercise any of these rights you must: submit your request in writing to the facility's Administrator, provide a reason for your request and, if applicable, clearly indicate the action you want the facility to take. We may charge a fee for the costs of copying, mailing or other supplies associated with your request. We will notify you of the cost involved and you may choose to change or take back your request at that time before any costs are incurred.***

## CHANGES TO THIS NOTICE

We reserve the right to change this notice. We reserve the right to make the revised or changed notice effective for medical information we already have about you as well as any information we receive in the future. We will post a copy of the current notice in the facility and on the website. In addition, if material changes are made to this notice, the notice will contain an effective date for the revisions and copies can be obtained by contacting the facility's Administrator.



## COMPLAINTS

If you believe your privacy rights have been violated, you may file a complaint with the facility or with the Secretary of the Department of Health and Human Services. To file a complaint with the facility, contact the Administrator or you may call the InTouch Hotline at 1(800) 255-4730 to report your concerns. All complaints to the facility's Administrator must be submitted in writing. **You will not be penalized for filing a complaint**.

**SUBJECT: AMENDMENT AND CORRECTION TO PROTECTED HEALTH INFORMATION (PHI)/MEDICAL RECORD**

## POLICY:

Patients/residents have the right to request an amendment to the protected health information (PHI) contained in the designated record set as specified in the Notice of Privacy Practices. The Facility has the right to refuse to amend the PHI. If the request is denied, the Facility will provide a written denial to the patient/resident.

## DEFINITIONS:

**Protected Health Information (PHI):** Is defined as individually identifiable health information that is maintained or transmitted by a healthcare provider in any form, including electronic records, paper records and oral discussions. Some examples of protected health information are interdisciplinary progress notes, physician's orders, care plans and billing information that contains patient/resident health information.

***Designated Record Set:*** *A group of records maintained by the facility that consists of the medical records and billing records for the patient/resident and that is used by the facility to make decisions about the patient/resident. The designated record set includes billing information that may contain ICD-9-CM codes that represent conditions of the patient/resident and are protected health information.*

## PROCEDURES:

1. Requests for an amendment of PHI are referred to the Privacy Designee or his/her designee.

2. When a patient/resident or the legal representative requests an amendment, provide the patient/resident with the **Request for Amendment of Protected Health Information (NFF-IP021P)** form available on the Fundamental Resource Center (FRC).
   A. A request is not evaluated until it is completed and signed by the patient/resident or the legal representative. The Privacy Designee or his/her designee may assist with completion of the form.

3. The **Request of Amendment of Protected Health Information** form is faxed to the Fundamental Administrative Services, LLC (FAS) Legal Department for approval by using the **Medical Records Request Fax Cover Sheet** in the Disclosure of Protected Health Information (PHI) Medical Records policy.

4. After the completed request form is received, log the request on the **HIPAA Request and Response Log** under the "HIPAA" tab in the patient's/resident's medical record. (See **HIPAA Documentation** policy.)

**SUBJECT: AMENDMENT AND CORRECTION TO PROTECTED HEALTH INFORMATION (PHI)/MEDICAL RECORD (Continued)**

5. Responding to the Request to Amend PHI:
   A. After a completed request form is received, there is a limit of sixty (60) days to act on the request.
   B. There is a one-time extension of no more than thirty days.
      1) Notify the patient/resident of the extension, the reason for the extension and the date by which action is taken by completing the **Request for Amendment Notification of Time Extension (NFF-IP022P)** form available on the FRC and provide the form to the patient/resident for his/her signature
      2) A copy of the **Request for Amendment Notification of Time Extension** form is provided to the patient/resident and the original form is filed under the "HIPAA" tab in the patient's/resident's medical record.
   C. Review the completed request form and refer it to Clinical Supervisor or his/her designee. The Clinical Supervisor or his/her designee in consult with appropriate disciplines and/or the Medical Director reviews the request and determines whether or not to accept the requested amendment.

6. A request to amend PHI may be denied, if it is determined that the PHI:
   **A. Was not created by the Facility.** An exception may be granted if the patient/resident provides a reasonable basis to believe that the creator of the PHI is no longer available to act on the requested amendment and it is apparent that the amendment is warranted.
      1) For example, a hospital or clinic which has given the Facility information on a patient/resident and has since closed its doors and left no means of obtaining its past information or records that were destroyed by fire or flood with no backup copies available. **This should rarely be the case. Every other avenue is to be explored before an amendment is made to information that was not created by the Facility.**
   **B. Is not part of the designated record set.** For example, information that is gathered on worksheets or daily communication sheets that do not become a part of the medical record and are not retained.
   **C. Would not be available for inspection under 45 CFR § 164.524 of the Privacy Regulations.**
   D. For example, psychotherapy notes which are not part of the Designated Record Set. **Contact the Privacy Officer for additional information.**
   **E. Is accurate and complete.**

**Denial of the Request to Amend**

1. If it is determined in consultation with the Clinical Supervisor or his/her designee, that the request for amendment is denied in whole or in part, notify the patient/resident of the denial by completing the **Notice of Denial of Request for Amendment of Medical Information (NFF-IP023P)** form available on the FRC.

**SUBJECT: AMENDMENT AND CORRECTION TO PROTECTED HEALTH INFORMATION (PHI)/MEDICAL RECORD (Continued)**

2. The patient/resident may submit a written Statement of Disagreement
   A. If the patient/resident submits a written Statement of Disagreement, a written rebuttal may be prepared by the Facility may be prepared. A copy of the written rebuttal is provided to the patient/resident.

3. Document the denial by placing a reference as close to the PHI that is the subject of the disputed amendment as possible (for example, write in the margin that the "*Amendment Denial is filed under the HIPAA tab*") and file the following documentation under the "HIPAA" tab in the patient's/resident's medical record:
   A. The patient's/resident's Request for Amendment of PHI form;
   B. The Facility's Notice of Denial form;
   C. The patient's/resident's Statement of Disagreement, if any; and
   D. The Facility's written rebuttal, if any.

4. Log the denial on the **HIPAA Request and Response Log** under the "HIPAA" tab in the patient's/resident's medical record.

5. Future Disclosures of PHI that is the Subject of the Disputed Amendment
   A. If the patient/resident submitted a Statement of Disagreement, disclose all information listed in Step 8 above or an accurate summary of such information with all future disclosures of the PHI to which the disagreement relates.
   B. If the patient/resident did not submit a Statement of Disagreement but did check "Yes" on the **Notice of Denial of Request for Amendment of Medical Information** to request that the **Request for Amendment of PHI** form and the **Notice of Denial of Request for Amendment of Medical Information** form be provided with any future disclosures, include these documents (or an accurate summary of that information) with all future disclosures of the PHI to which the disagreement relates.

**Acceptance of the Request to Amend**

1. If it is possible, amend the PHI in the patient's/resident's medical record. If it is not possible to amend the PHI, provide a reference as close to the PHI as possible (for example, write in the margin that the "*Amendment to this documentation is filed under the HIPAA tab*") and file the amendment under the "HIPAA" tab in the patient's/resident's medical record.

2. Log the acceptance on the **HIPAA Request and Response Log** under the "HIPAA" tab in the patient's/resident's medical record.

3. Notify the patient/resident of the amendment by completing the **Notice of Acceptance of Request for Amendment of Medical Information (NFF-IP024P)** form available on the FRC.

**SUBJECT: AMENDMENT AND CORRECTION TO PROTECTED HEALTH INFORMATION (PHI)/MEDICAL RECORD (Continued)**

4. Have the patient/resident indicate on the form the names of any persons or organizations with which the amendment needs to be shared. (An example might be a clinic that was previously given the information for continued treatment.)

5. The Facility makes reasonable efforts to provide the amendment to:
   A. Persons identified by the patient/resident on the **Notice of Acceptance of Request for Amendment of Medical Information** form; and
   B. Persons, including business associates, known to have received the PHI that is in need of amendment and that may have relied or could foresee ably rely on such information to the detriment of the patient/resident.
   C. Notify those identified via mail by completing the **Notification of Amendment of Medical Information (NFF-IP025P)** form available on the FRC. File copies of these notifications under the "HIPAA" tab in the patient's/resident's medical records.

6. If another health care provider notifies the Facility of an amendment, document the amendment in the patient's/resident's medical record.
   A. If it is possible, amend the PHI in the patient's/resident's medical record. If it is not possible to amend the PHI, provide a reference as close to the PHI as possible (for example, write in the margin that the "*Amendment to this documentation is filed under the HIPAA tab*") and file the amendment under the "HIPAA" tab in the patient's/resident's medical record.

**REFERENCES:**

**1. HIPAA Final Privacy Regulations:**
45 CFR § 164.520
45 CFR § 164.524
45 CFR § 164.526
45 CFR § 164.530

## SUBJECT: ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

## POLICY:

1. A patient/resident or the patient's/resident's legal representative has a right to receive an accounting of disclosures of Protected Health Information (PHI) maintained in his or her designated record set, as stated in the *Notice of Privacy Practices*. This policy documents the process for responding to a patient's/resident's request for an accounting of disclosures of their protected health information made by the Facility. The requested information will not include protected health information released or disclosed on or prior to April 13, 2003.
2. Disclosures will be retained for no less than a six-year period.

## DEFINITIONS:

**Protected Health Information (PHI):** Is defined as individually identifiable health information that is maintained or transmitted by a healthcare provider in any form, including electronic records, paper records and oral discussions. Some examples of protected health information are interdisciplinary progress notes, physician's orders, care plans and billing information that contains patient/resident health information.

**Designated Record Set:** A group of records maintained by the facility that consists of the medical records and billing records for the patient/resident and that is used by the facility to make decisions about the patient/resident. The designated record set includes billing information that may contain ICD-9-CM codes that represent conditions of the patient/resident and are protected health information.

**Qualified Exceptions to the Accounting**

1. The disclosure was necessary to carry out treatment, payment, and health care operations.
2. The disclosure was to the patient/resident for which the PHI was created or obtained, e.g. the patient/resident.
3. The disclosure was pursuant to a signed authorization by the patient/resident or legal representative.
4. The disclosure to persons involved in the patient's/resident's care pursuant to the patient's/resident's consent or for other notification purposes.
5. The disclosure was for national security or intelligence purposes.
6. The disclosure was to a correctional institution.
7. The disclosure was temporarily suspended by a law enforcement official or health oversight agency.
8. Incidental disclosures.
9. As part of a Limited Data Set (LDS).
10. The disclosure occurred on or prior to April 13, 2003.

**SUBJECT: ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION (Continued)**

**Potential Areas where Accounting of Disclosures Applies**

1. ***Disclosures to Public Health Authorities***
   - A. For the purpose of preventing or controlling disease, injury or disability
   - B. To conduct public health surveillance
   - C. For public health investigations and interventions
   - D. For reporting vital events such as births and deaths
   - E. To a foreign government agency at the request of a public health authority
   - F. To report child/elder abuse
   - G. If necessary, to prevent or lessen a serious and imminent threat to the health or safety of an patient/resident or the public
2. ***Disclosures to an Entity Subject to the Food and Drug Administration***
   - A. To report adverse events, product defects or biological product deviations
   - B. To track products
   - C. To enable product recalls, repairs or replacements
   - D. To conduct post marketing surveillance
3. ***Disclosures to an Employer***
   - A. Only PHI specific to a work-related illness or injury, and
   - B. Required for the employer to comply with its obligations under federal or state occupational safety and health laws
4. ***Disclosures to Health Oversight Agencies***
   - A. State Surveys, annual or complaint
   - B. Office of Inspector General (OIG) investigations
   - C. For government benefit program eligibility
   - D. To determine compliance with civil rights laws
   - E. For civil, administrative or criminal investigations, proceedings or actions
5. ***Disclosures in Judicial and Administrative Proceedings***
   - A. In response to a court order or court ordered warrant
   - B. In response to a subpoena, only if approved by the Fundamental Administrative Services, LLC (FAS) Legal Department
6. ***Disclosures to Law Enforcement Officials***
   - A. For the purpose of locating a suspect, fugitive, material witness or missing person
   - B. About a patient/resident who is or is suspected to be a victim of a crime
   - C. Regarding crimes on the Facility premises
   - D. Regarding suspicious deaths
   - E. In response to an administrative request, civil investigative demand or grand jury subpoena, after review by the FAS Legal Department
   - F. For the purpose of averting a serious threat to health or safety
7. ***Disclosures about victims of abuse, neglect or domestic violence***
   - A. To a government authority authorized by law to receive reports of abuse, neglect or domestic violence
8. ***Disclosure of Deceased Persons' PHI***
   - A. To the Coroner, Medical Examiner
   - B. For organ procurement organizations

**SUBJECT: ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION (Continued)**

9. ***Disclosures for Specialized Government Functions***
   - A. To Armed Forces personnel for military purposes
   - B. To authorized federal officials for the protection of the President and other federal officials
   - C. To other government agencies, if approved by the FAS Legal Department

10. ***Disclosures for Worker's Compensation***
   - A. As authorized by and to the extent necessary to comply with the law

11. ***Other Activities as Required By Law***

**PROCEDURES:**

1. Requests for an accounting of disclosures of PHI are referred to the Privacy Designee or his/her designee.

2. When a patient/resident requests an accounting of disclosures, provide the patient/resident with the **Request for an Accounting of Disclosures of PHI (NFF-IP026P)** form available on the Fundamental Resource Center (FRC)**.**
   - A. A request is not evaluated until it is completed and signed by the patient/resident or the legal representative. The Privacy Designee or his/her designee may assist with completion of the form.

3. The **Request for Accounting of Disclosures of PHI** form is faxed to the FAS Legal Department for approval by using the **Medical Records Request Fax Cover Sheet** in the Disclosure of Protected Health Information (PHI)/Medical Records policy.

4. After approval is received from the FAS Legal Department, log the request on the **HIPAA Request and Response Log** under the "HIPAA" tab in the patient's/resident's medical record. (See **HIPAA Documentation** policy.) The Privacy Designee or his/her designee reviews and processes the request.

5. Time frames for responding to the Request for an Accounting:
   - A. After the completed request form is received, there is a limit of sixty (60) days to act on the request, unless state or other federal law requires a shorter timeframe.
   - B. There is a one-time extension of no more than thirty days.
     1) Notify the patient/resident of the extension, the reason for the extension and the date by which action is taken by completing the **Accounting of Disclosure Request Notification of Time Extension (NFF-IP027P)** form available on the FRC and provide the form to the patient/resident for his/her signature.
     2) A copy of the Accounting of Disclosure Request Notification of Time Extension form is provided to the patient/resident and file the original form under the "HIPAA tab in the patient's/resident's medical record.

**SUBJECT: ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION (Continued**

6. A written accounting is provided to the patient/resident using the **Accounting of Disclosures (NFF-IP028P)** form available on the FRC.
   A. The accounting includes disclosures during the period specified in the request. The specified period may be up to six years prior to the date of the request, but not on or before April 13, 2003. )
   B. The Facility includes known disclosures made by its business associates, if aware of those disclosures.
   C. Compare the **HIPAA Correspondence Log** in the HIPAA binder or folder in the against the **HIPAA Request and Disclosure Table** for any accountable disclosures. (See **Disclosure of Protected Health Information (PHI)/Medical Records** policy.)
   D. State Surveys and OIG audits/investigations are accountable disclosures. If such disclosures have taken place during the time period specified in the request, those disclosures are included in the accounting.
      1) If specific information regarding these disclosures is not available, document the following on the **Accounting of Disclosures** form:
         a) The name of the entity or person to whom PHI was disclosed (if the specific name is not available, "State surveyor" or "OIG auditor" is acceptable),
         b) The address of such entity or person, if known,
         c) A brief description of the PHI that was disclosed, ("Access to entire medical record" is acceptable, if specific access is not known.)
         d) A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, and
         e) The date of the disclosure
   E. Review the **Accounting of Disclosures** form with the Clinical Supervisor or his/her designee to determine if any of the following disclosures were made regarding the patient/resident during the requested time period:
      1) Incidents reported to the State or other authority.
      2) Abuse reports to the State or other authority.
      3) Reporting to public health authorities.
   F. Disclosures that qualify as an exception as described above are excluded from the accounting.
   G. For each accountable disclosure, document the following on the **Accounting of Disclosures** form:
      1) the name of the entity or person to whom PHI was disclosed,
      2) the address of such entity or person, if known,
      3) a brief description of the PHI that was disclosed,
      4) a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, and
      5) the date of the disclosure.

**SUBJECT: ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION (Continued)**

H. If there are multiple disclosures for health oversight or law enforcement officials for a single purpose, you may provide:
   1) the first disclosure during the accounting period;
   2) the frequency, or number of disclosures made during the accounting period; and
   3) the date of the last such disclosure during the accounting period.

7. The first accounting to a patient/resident within a 12-month period is provided without charge. However, a reasonable, cost-based fee may be imposed for each subsequent request for an accounting by the same patient/resident within the 12-month period, provided that the patient/resident is informed of the charges, in advance, and is given the opportunity to withdraw or modify the request.

8. Once the **Accounting of Disclosures** form has been provided to the patient/resident, log the request on the **HIPAA Request and Response Log** under the "HIPAA" tab in the patient's/resident's medical record. File a copy of the **Accounting of Disclosures** form under the HIPAA tab in the patient's/resident's medical record.

9. The following documentation related to the request for an accounting of disclosures is retained for no less than six (6) years from the date of the accounting:
   A. The information required to be included in the accounting, and
   B. The written accounting provided to the requesting party.

**REFERENCES:**

1. **HIPAA Final Privacy Regulations:**
   45 CFR § 164.528
   45 CFR § 164.530

## SUBJECT: RESTRICTION OF PROTECTED HEALTH INFORMATION

**POLICY:**
A patient/resident or patient's/resident's legal representative has the right to request restrictions for the uses and disclosures of Protected Health Information (PHI), as stated in the *Notices of Privacy Practices*.

The Facility is not required to accept such a request, but will review each request to determine whether to accept or deny the request, considering the need for access to PHI for treatment and payment purposes.

**DEFINITIONS:**

**Protected Health Information (PHI):** Is defined as individually identifiable health information that is maintained or transmitted by a healthcare provider in any form, including electronic records, paper records and oral discussions. Some examples of protected health information are interdisciplinary progress notes, physician's orders, care plans and billing information that contains patient/resident health information.

**PROCEDURES:**

1. The Privacy Designee or his/her designee manages the requests for restrictions of Protected Health Information (PHI).

2. Upon receiving a request to restrict the use or disclosure of PHI from a patient/resident or the legal representative, Privacy Designee or his/her designee provides the patient/resident or the legal representative with the **Request to Restrict Use and Disclosure of Protected Health Information (NFF-IP030P)** form available on the Fundamental Resource Center (FRC).

3. A request to restrict PHI is not evaluated until the request form is complete and signed by the patient/resident or the legal representative. Privacy Designee or his/her designee may assist with completion of the form.

4. Upon receiving a completed request form, log the receipt on the **HIPAA Request and Response Log** under the "HIPAA" tab in the patient's/resident's medical record. (See **HIPAA Documentation** policy.)

5. The Privacy Designee or his/her designee consults with appropriate staff to review the request in order to determine if the request negatively impacts the patient's/resident's treatment or the Facility's ability to receive payment for services.

   The Facility **must agree** to a patient's/resident's or legal representative's request to restrict the disclosure of their PHI to their health plan if they pay for the item(s) or service(s) in full. This does not apply to submissions that are required by state and/or federal regulations. Contact the Fundamental Administrative Services, LLC Privacy and Security Officer for further guidance.

6. After a review of the request, complete the form by either checking "Agrees to" or "Declines to" in the Notification section on the **Request to Restrict Use and Disclosure of Protected Health Information** form. The Privacy Designee's or Clinical Supervisor's signature is required on this form.

**SUBJECT: RESTRICTION OF PROTECTED HEALTH INFORMATION (Continued)**

7. Provide a copy of the completed form to the patient/resident notifying them of the decision.

8. Log the response on the **HIPAA Request and Response Log** under the "HIPAA" tab in the patient's/resident's medical record.

9. File the original hard copy of the request and response in the patient's/resident's medical record under the "HIPAA" tab.

**Restriction Accepted**

1. If the requested restriction is agreed to, place a "**Confidential Information**" sticker (L-2077) on the cover of the chart.

2. Notify appropriate Facility staff that is impacted by the restriction.

3. The Facility abides by the accepted restriction with the following exceptions:
   A. The Facility may use the restricted PHI, or may disclose such information to a health care provider if:
      1) The patient/resident is in need of emergency treatment, and
      2) The restricted PHI is needed to provide the emergency treatment.
      In this case, the Facility can release the information but advises the emergency treatment provider not further use or disclose the patient's/resident's PHI.
   B. When required by the Secretary of Health and Human Services to investigate or determine the Facility's compliance with the Privacy Rule; and
   C. When legally required to use and disclose by law. (These uses and disclosures are detailed in the **Notice of Privacy Practices**.)

**Terminating the Restriction**

Termination Initiated or Agreed to by the Patient/Resident

1. If the patient/resident or the legal representative requests that the restriction be terminated, the Privacy Designee or his/her designee provides the patient/resident with the **Notification of Termination of the Restriction** form for completion and execution. A copy of the completed for is returned to the patient/resident.

2. The Privacy Designee or his/her designee documents the termination of the restriction on the **HIPAA Request and Response Log** in the patient's/resident's medical record and file the **Notification of Termination of the Restriction (NFF-IP031P)** form available on the FRC in the patient's/resident's medical record under the "HIPAA" tab.

3. Remove the "**Confidential Information**" sticker from the cover of the chart.

**SUBJECT: RESTRICTION OF PROTECTED HEALTH INFORMATION (Continued)**

4. Termination of a restriction with the patient/resident's agreement is effective for all PHI created or received by the Facility since the date of admission.

5. The Privacy Designee or his/her designee notifies the appropriate Facility staff of the termination of the restriction.

Termination Initiated by the Facility

1. If a staff member wishes to terminate a restriction place on a patient's/resident's file, bring your request to the Privacy Designee or Clinical Supervisor for approval. All requests for termination of a restriction are approved by the Privacy Designee or Clinical Supervisor.

2. To terminate the restriction, HIM staff notify the patient/resident by completing and providing the **Notification of Termination of the Restriction** form to the patient/resident for his/her consent or dissent.

3. If the patient/resident agrees to the termination of the restriction, the restriction is lifted for all PHI created or received by the Facility.

4. If the patient/resident does not agree to the termination of the restriction, the termination only applies to PHI created or received after the Facility has informed the patient/resident of the termination and the Facility continues to abide by the restriction with respect to any PHI created or received before it informed the patient/resident of the termination of the restriction.

5. The Privacy Designee or his/her designee documents the termination of the restriction on the **HIPAA Request and Response Log** in the patient's/resident's medical record.

6. The Privacy Designee or his/her designee provides a copy of the duly executed and completed **Notification of Termination of Restriction** form to the patient/resident or legal representative and place the **Notification of Termination of Restriction** form under the "HIPAA" tab in the patient's/resident's medical record.

**REFERENCES:**

1. **HIPAA Final Privacy Regulations**

45 CFR § 164.520
45 CFR § 164.522(a)
45 CFR § 164.601

## SUBJECT: COMMUNICATIONS BY ALTERNATIVE MEANS/LOCATION

### POLICY:

A patient/resident will be allowed to request that the Facility communicate PHI to him/her by alternative means or at alternative locations. The Facility will accommodate reasonable requests.

### DEFINITIONS:

**Protected Health Information (PHI):** Is defined as individually identifiable health information that is maintained or transmitted by a healthcare provider in any form, including electronic records, paper records and oral discussions. Some examples of protected health information are interdisciplinary progress notes, physician's orders, care plans and billing information that contains patient/resident health information.

### PROCEDURES:

1. Patients/Residents are notified of the right to request communication by alternative means or at alternative locations in the **Notice of Privacy Practices**.

2. The Privacy Designee or his/her designee manages the requests to receive communications by alternative means.

3. When a patient/resident requests that the Facility communicate with the him/her or his/her legal representative by some alternate means, the Privacy Designee or his/her designee provides the patient/resident with a copy of the **Request for Communications by Alternative Means (NFF-IP029P)** form available on the Fundament Resource Center (FRC).

Note: A request is not evaluated until this request form is completed and signed by the patient/resident or legal representative.

4. Upon receiving a completed request form, log the receipt on the **HIPAA Request and Response Log** under the "HIPAA" tab in the patient's/resident's medical record. (See **HIPAA Documentation** policy.)

5. Review the request form with appropriate staff to determine if it is a reasonable request.
   A. The Facility may not require an explanation for the request.
   B. The Facility's decision is not based on the perceived merits of the request.
   C. The Facility accommodates a request determined to be reasonable.

6. After a review of the request, complete the form either by checking "Agrees to" or "Declines to" on the **Request for Communications by Alternative Means** form. If the request is declined, provide the reason in the space provided on the form.

7. Provide a copy of the completed form to the patient/resident notifying them of the decision.

**SUBJECT:** **COMMUNICATIONS BY ALTERNATIVE MEANS/LOCATION (Continued)**

8. Log the response on the **HIPAA Request and Response Log** under the "HIPAA" tab in the patient's/resident's medical record.
9. File the original hard copy of the request and response in the patient's/resident's medical record under the "HIPAA" tab.
10. If the request is accepted, notify appropriate departments that are impacted by this request.

**REFERENCES:**

1. **HIPAA Final Privacy Regulations**

   45 CFR §164.522(b)(1)

## SUBJECT: MARKETING COMMUNICATIONS

## POLICY:

1. Marketing communications will comply with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule's specific requirements as well as any applicable State laws. The patient's/resident's protected health information will be safeguarded while also allowing patients/residents to receive materials that would in their best interest.
2. Marketing communications, as defined by the HIPAA Privacy Rule, will require a prior written authorization from the patient/resident.

## DEFINITIONS:

**Marketing**: Marketing is a communication about a product or service that encourages recipients of the communication to buy or use the product or service.
Marketing does not include a communication made:

(i) To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entities cost of making the communication.
(ii) For the following treatment and health care operations purposes, **except where the covered entity receives financial remuneration in exchange for making the communication**:

(A) For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;
(B) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or
(C) For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

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

**Protected Health Information (PHI):** Is defined as individually identifiable health information that is maintained or transmitted by a healthcare provider in any form, including electronic records, paper records and oral discussions. Some examples of protected health information are interdisciplinary progress notes, physician's orders, care plans and billing information that contains patient/resident health information.

## PROCEDURES:

### Marketing Disclosures Outside of the Facility

1. If the Facility is using or disclosing PHI in conjunction with a marketing communication, the patient/resident or their legal representative signs an authorization prior to the communication. The Fundamental Administrative Services, LLC (FAS) Legal Department is consulted before new marketing programs that involve patients/residents are instituted.

2. The FAS Legal Department provides the proper authorizations and releases for the marketing program. If the marketing involves direct or indirect compensation to the Facility from a third party, the authorization states that such third-party compensation is involved.

### Marketing to a Patient/Resident

1. The marketing restrictions apply only if the Facility is using PHI in conjunction with a marketing communication.

2. The patient's/resident's authorization is required if the Facility receives financial remuneration in exchange for making a marketing communication from or on behalf of a third party whose product or service is being described.

3. Exceptions:
   The patient's/resident's authorization is not required, even if the Facility receives financial remuneration, if the marketing communication consists of a:
   A. Face-to-face communication made by the Facility to the patient/resident. A communication made over the phone is not considered face-to-face.
   B. Promotional gift of nominal value from a vendor provided by the Facility to the patient/resident.
   C. Communication directed at an entire population rather than to a targeted patient/resident, that promotes health in a general manner and do not endorse a specific product or service.
   D. Communication to remind a patient/resident of a refill or otherwise communicate about a drug or biologic that is currently being prescribed for the patient/resident, only if any financial remuneration received by the Facility in exchange for making the communication is reasonably related to the Facility's cost of making the communication.

4. When the Facility receives financial remuneration for a marketing communication anti-kickback, fraud and abuse or self-referral statutes and regulations may apply and are considered. The Facility should contact the FAS Legal Department for guidance regarding these statutes and regulations.

## REFERENCES:

1. **HIPAA Final Privacy Regulations**
   45 CFR § 164.501; 45 CFR § 164.508

## SUBJECT: DESIGNATED RECORD SET FOR PROTECTED HEALTH INFORMATION

**POLICY:**
The Health Insurance Portability and Accountability Act (HIPAA) provide that requests for access to protected health information specifically identify the information to be inspected, amended and/or copied. Requests for access to protected health information will be limited to that which is contained within the provider's Designated Record Set.

**DEFINITIONS:**

**Protected Health Information (PHI):** Is defined as individually identifiable health information that is maintained or transmitted by a healthcare provider in any form, including electronic records, paper records and oral discussions. Some examples of protected health information are interdisciplinary progress notes, physician's orders, care plans and billing information that contains patient/resident health information.

**Designated Record Set:** A group of records maintained by the facility that consists of the medical records and billing records for the patient/resident and that is used by the facility to make decisions about the patient/resident. The designated record set includes billing information that may contain ICD-9-CM codes that represent conditions of the patient/resident and are protected health information.

**Legal Medical Record**: The Legal Medical Record documents the health care services provided to a patient/resident in any aspect of health care delivery by a provider. The Legal Health Record is individually identifiable data, collected and used in documenting healthcare services rendered. The term includes records of care used by healthcare professionals while providing patient/resident care services, for reviewing patient data, or documenting observations, actions, or instructions. The Legal Medical Record is included as part of the designated record set.

**Patient Financial Records:** Patient Financial records represents admission and financial information about our patients/residents and is included as part of the Designated Record Set.

**Personal Health Records:** Personal Health Records are hard copy of the patient's/resident's personal health information provided to the facility by the patient/resident or responsible party. These records may be hard copies of records that are maintained on line by the patient/resident or responsible party. If such records are used by Providers to make patient health care related decisions, and to provide patient care services, review patient data, or document observations, actions or instructions then records will be considered part of the **Designated Record Set.**

**SUBJECT: DESIGNATED RECORD SET FOR PROTECTED HEALTH INFORMATION (Continued)**

**LEGAL MEDICAL RECORD**

| Included Items in the Designated Record Set | **Form Supplied to Patient/resident** | Source |
|---|---|---|
| The Legal Medical Record is comprised of source data incorporated into progress notes, including:<br>• Care Plan<br>• History and Physical<br>• Physician Orders<br>• Interdisciplinary Progress Notes<br>• Consultation Reports<br>• Assessment Flow sheets<br>• Behavior/Emotional Pattern Flow Sheets and Reports<br>• Clinical Management Records<br>• Elimination Records<br>• Nutrition/Eating Records<br>• Physical Functioning Records<br>• Psychotropic Drug Utilization Records<br>• Quality of Life Records<br>• Skin Care Records<br>• Diagnostic Records<br>• MED/TX Records<br>• Legal and Consent Records<br>• Interdisciplinary Discharge Summary<br>• Physician Discharge Summary<br>• Post-Discharge Plan of Care<br>• Minimum Data Set specific to patient/resident * | • Copy of paper chart, printout, or summarization,<br>• View computer screen or original record with attendant only | Physician, Charge Nurse, Medical Records Department |

* Excluded from the Designated Record Set is all source data, including photographs, films, monitoring strips, videotapes, slides, and worksheets.

If records from other providers are used by the Facility to make decisions related to the care and treatment of the patient/resident then these records are considered part of the Designated Record Set as well as the Legal Medical Record, e.g., history and physical, discharge summary and labs from previous acute care hospitalization.

**SUBJECT: DESIGNATED RECORD SET FOR PROTECTED HEALTH INFORMATION (Continued)**

**PATIENT FINANCIAL RECORDS**

| Included Items in the Designated Record Set | Form Supplied to Patient/resident | Source |
|---|---|---|
| Patient-specific claim, remittance, eligibility response, and claim status response, statement of account balance, and payment agreement | Copy of paper document or printout only | Business Office |
| Consent and authorization forms, Medicare Letters e.g. Life Time Reserve Letter and Notice of Non-Coverage Letter, and copy of insurance card | Copy of paper document only | Business Office, Medical Records Department |

**PERSONAL HEALTH RECORD**

| Included Items in the Designated Record Set | Form Supplied to Patient/resident | Source |
|---|---|---|
| Patient-submitted documentation and referral letters * | Copy of paper chart or printout, computer screen or original record with attendant only | Medical Records Department, Administrative Nursing Personnel, Privacy Officer |

* Excluded from Designated Record Set, unless used by the Facility to make decisions related to the care and treatment of the patient/resident.

**OTHER/ADMINISTRATIVE DATA**

* Excluded from Designated Record Set: Administrative data, such as audit trails, appointment schedules, and practice guidelines that do not imbed patient data. Also excluded are incident reports, quality assurance data and vital certificate worksheets and derived data such as:

- Accreditation reports
- Anonymous patient data for research purposes
- Public health records
- Statistical report

## SUBJECT: ACCESS REQUEST POLICY

## POLICY:

Facility information and resources are used only for appropriate business purposes. All employees, contractors, consultants, and students are aware of their obligations to protect Facility information and resources.

Facility information is not to be accessed by or disclosed to anyone who does not need the information to perform the activities and fulfill the responsibilities associated with his or her role in the Facility. Facility resources are not accessed or used by anyone who does not need the resource in order to perform the activities and fulfill the responsibilities associated with his or her role in the Facility.

Employees, contractors, consultants, and students authorized to access Facility information are responsible for properly storing and securing it from unauthorized access, as well as for securing and protecting passwords, keys, and other forms of access control. Employees, contractors, consultants, and students authorized to access Facility resources are required to use them responsibly and in compliance with policy and procedure.

Those authorized to grant or revoke access to Facility information and resources (as specified below) are responsible for following procedures to ensure that access is appropriately assigned, modified as needed, and terminated promptly when employees, contractors, consultants, and students transfer to other positions or leave the Facility.

Misuse of Facility information or resources is a violation of Facility policy. Violations of this policy are reported to the Administrator/Executive Director and the Fundamental Administrative Services, LLC (FAS) Privacy and Security Officer. The FAS Information Security Department disables access for any employee, contractor, consultant, or student found to be accessing Facility information or resources in violation of policy and procedure. Sanctions for violations of this policy include disciplinary action up to and including termination.

Additionally, there are certain categories of information, such as Protected Health Information that are covered by the Health Insurance Portability & Accountability Act (HIPAA) when used by a covered entity. Anyone who violates state or federal law is personally liable for such actions under the law as well as under Facility policy.

## PROCEDURES:

**Request to Grant Access to Facility Information and Resources**

1. The following managerial roles (Authorized Requestors) are authorized to request, modify or revoke access to Facility information and resources:
   A. The Administrator/Executive Director requests access to Facility information and resources for all employees, contractors, consultants, and students.
   B. The Director of Nursing (DON)/Clinical Manager requests access to clinical Facility information and resources for clinical employees, contractors, consultants, and students.

**SUBJECT: ACCESS REQUEST POLICY (Continued)**

C. The Business Office Manager requests access to Facility information and resources for non-clinical employees, contractors, consultants, and students.

D. The Administrator/Executive Director may limit the DON's/Clinical Manager's and BOM's authority to request access by notifying the FAS Information Security Department.

2. Authorized Requestors request the minimum amount of access to Facility information and resources as necessary for the employees, contractors, consultants, and students to perform their functions at the Facility.

3. Prior to requesting access for contractors, consultants, and students, the Administrator/Executive Director is responsible for verifying that a written agreement and business associate agreement, where applicable, has been executed. All such agreements are forwarded to the FAS Legal Department for review prior to execution.

4. To request access, Authorized Requestors complete the Facility System Access Request Form (FSARF) on the Fundamental Resource Center and submit it to the FAS Information Security Department. The FAS Information Security Department processes the request within 24 hours but may take up to 5 business days to complete the request.

5. If an employee other than one of the Authorized Requestors completes the FSARF, the FAS Information Security Department forwards the request via email to an Authorized Requestor for approval. This will result in a delay in processing the request.

6. In some cases, requests may be forwarded to the Fundamental Clinical and Operational Services, LLC Regional or Divisional Vice President for review and consultation. This may result in a delay in processing the request.

7. If required information is not included on the FSARF or the request requires further information, the FAS Information Security Department forwards the request via email to an Authorized Requestor to obtain the information. This will result in a delay in processing the request.

8. It is the responsibility of the Authorized Requestors to monitor their email for messages from the FAS Information Security Department regarding requests for access.

9. Once the requested access has been granted, the FAS Information Security Department forwards the user's login and password information to the Authorized Requestor. It is the Authorized Requestor's responsibility to distribute to the login and password information to the employee, contractor, consultant, or student.

**SUBJECT: ACCESS REQUEST POLICY (Continued)**

**Access to Facility Information and Resources**

1. Whenever possible, access should be as granular as feasible. Employees, contractors, consultants, and students should only have read or write access to the data required for performing their appropriate function. In most cases, access will fall into one of the following categories:
   - **A. update (read/write)** access: the ability to enter and update data and submit transactions; or
   - **B. lookup** (**read-only**) access: the ability only to view information without being able to enter or change data.

2. In some cases appropriate access may consist of read/write access to one portion of a database, read-only access to other portions and, potentially, no access to yet other portions.

**Modifications to Access to Facility Information and Resources**

1. Whenever the duties of an employee, contractor, consultant, or student change, an Authorized Requestor requests a change to access by completing and submitting the FSARF.
2. If an employee, contractor, consultant, or student no longer needs access to Facility information or resources (for instance, upon termination of employment or contract), it is the responsibility of an Authorized Requestor to request that access be terminated by completing and submitting the FSARF as soon as possible.

**This policy applies to all applications/systems accessed by Facility employees, contractors, consultants, and students, even in the very limited instances where access to the application/system is not administered by the FAS Information Security Department. It is the responsibility of the Administrator/Executive Director, Business Office Manager, and Director of Nursing/Clinical Manager to request and manage the proper access to all applications/systems.**

**REFERENCE:**

1. **HIPAA Final Privacy Regulations**

   164.308(a)(3)(C)
   164.308(a)(4)
   164.308(a)(4)(B)
   164.308(a)(4)(C)

## SUBJECT: SAFEGUARDING PROTECTED HEALTH INFORMATION

## POLICY:

Health Information Management (HIM) staff will set up access controls and physical safeguards to prevent prohibited uses and disclosures of Protected Health Information ("PHI") and limit incidental uses and disclosures of PHI in various media. Also see the *Safeguarding – Posted Protected Health Information* and *Safeguarding Electronic Protected Health Information* policies.

## PROCEDURES:

## GENERAL RULES

1. **SAFEGUARDS FOR VERBAL USES (For any meetings or conversations.)**
   - A. **Meetings during which PHI is discussed:**
     1) Specific types of meetings where PHI may be discussed include, but are not limited to:
        a) Daily Standup or Department Head meetings
        b) Interdisciplinary Plan of Care meeting
        c) Medicare meeting
        d) Quad Checks
        e) Family Care Conference
     2) Meetings are conducted in an area that is not easily accessible to unauthorized persons.
     3) Meetings are conducted in a room with a door that closes, if possible.
     4) Voices are kept to a moderate level to avoid unauthorized persons from overhearing.
     5) Only staff that has a "need to know" the information is present at the meeting. See the *Minimum Necessary Uses & Disclosures of Protected Health Information* policy in this manual.
     6) The PHI that is shared or discussed at the meeting is limited to the minimum amount necessary to accomplish the purpose of sharing the PHI.

   - B. **Telephone conversations:**
     1) Telephones used for discussing PHI are located in as private an area as possible.
     2) Staff members take **reasonable** measures to prevent unauthorized persons from overhearing telephone conversations involving PHI. Reasonable measures may include:
        a) Lowering the voice;
        b) Requesting that unauthorized persons step away from the telephone area;
        c) Moving to a telephone in a more private area before continuing the conversation; and
        d) Limiting the PHI shared over the phone to an amount necessary to accomplish the purpose of the use or disclosure.

**SUBJECT: SAFEGUARDING PROTECTED HEALTH INFORMATION (Continued)**

C. **In-Person conversations:**
1) In patient/resident rooms or treatment areas
2) With patient/resident/family in public areas
3) With authorized staff in public areas
a) Take reasonable measures to prevent unauthorized persons from overhearing conversations involving PHI. Such measures may include:
1.) Lowering the voice;
2.) Moving to a private area within the Facility; and
3.) If in a patient/resident room, pulling the privacy curtain.

2. **SAFEGUARDS FOR WRITTEN PHI**

All documents containing PHI (Medical and Business Office Records) are stored appropriately to reduce the potential for incidental use or disclosure. Documents are not easily accessible to any unauthorized staff or visitors.

A. **Active Records:**
1) Active Medical Records are stored in an area or manner that secures the records from unauthorized access but allows for staff providing care to access the records quickly and easily as needed.
2) Authorized staff reviews the Medical Record in Medical Records, unless it is signed out (See the attached log as a sample for the sign out log).
3) Active Medical Records are not left unattended or unsecured in areas where patients/residents, visitors and unauthorized individuals could easily view the records.
4) Medication Administration Records, Treatment Administration Records, report sheets and other documents containing PHI are not left open.
5) Only authorized staff reviews the Medical Records. All authorized staff reviewing Medical Records does so in accordance with the minimum necessary standards. Refer to *Exhibit A: Role Based Access to PHI,* in the *Minimum Necessary Uses & Disclosures of Protected Health Information* policy of this manual.
6) Medical Records are protected from loss, damage and destruction. See *Record Protection from Damage* policy in this manual.

B. **Active Business Office Files:**
1) Active Business Office Files are stored in a secure area that allows authorized staff access as needed.

C. **Protected Health Information Outside the Facility:**
**This does not apply to medical records. See the *Maintaining Record Control* policy.**
1) PHI is taken out of the Facility by employees on a limited basis, in compliance with the minimum necessary requirements, and with prior approval of the Administrator.
2) PHI is returned to the Facility as soon as possible or is appropriately destroyed when no longer needed in compliance with the *Document Management Policy*. See *Destruction of Paper Documentation* below.
3) PHI is safeguarded from unauthorized access while in transit and at destination. PHI is not visible and is maintained in a secure manner such as a locked vehicle.

**SUBJECT: SAFEGUARDING PROTECTED HEALTH INFORMATION (Continued)**

3. **OFFICE EQUIPMENT SAFEGUARDS**

A. **Printers, copiers and fax machines:**

Also see POLICY: *Faxing of Protected Health Information* in this manual.

1) Fax machines and printers are located in areas not easily accessible to unauthorized persons.

If equipment cannot be relocated to a secure location, post a sign near the equipment indicating that unauthorized persons are prohibited from viewing documents from the equipment. Sample language: "Only authorized staff may view documents generated by this (indicate printer, copier, fax, etc). Access to such documents by unauthorized persons is prohibited by federal law."

2) Documents containing PHI are promptly **removed from the printer, copier or fax machine and placed in a**n appropriate and secure location.

3) Documents containing PHI that are disposed of due to an error in printing are destroyed by shredding or by placing the document in a secure shredding bin until destroyed.

4. **DESTRUCTION OF PAPER CONTAINING PHI**

A. PHI that is not part of the Medical Record and does not become part of the Medical Record (e.g., report sheets, shadow charts or files, notes, lists of vital signs, weights, billing reports, etc.) is destroyed promptly when it is no longer needed in accordance with the *Document Management* policy by shredding or placing the information in a secure recycling or shredding bin until the time that it is destroyed.

B. Follow the *Information Destruction* policy in this manual for closed records scheduled to be destroyed.

**REFERENCES:**

1. **HIPAA Final Privacy Regulations**
45 CFR § 164.530

## Sign Out Log of Records

| Date | Name on Chart | Time Removed | Person Removing Chart | Time Returned |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## SUBJECT: SAFEGUARDING ELECTRONIC PROTECTED HEALTH INFORMATION

**POLICY:**

All employees safeguard electronic protected health information in an effort to fulfill their duty to maintain the confidentiality and integrity of patient/resident health information as required by law, professional ethics and accreditation requirements. Access to and the use and disclosure of electronic protected health information is limited to the minimum necessary to fulfill the employee's obligations and duties. When accessing systems or applications that contain electronic protected health information including systems or applications administered by health plans or other providers; the following procedures must be followed. Whenever possible, the de-identified information will be used.

**DEFINITIONS:**

**Hardware** - the mechanical, magnetic, electronic, and electrical components making up a computer system where data and software are stored as well as where output is generated. Examples include but are not limited to personal computers, laptops, routers, wireless routers, printers, mobile devices and removable media.

**Mobile Devices** - a pocket-sized computing device, typically having a display screen with touch input or a miniature keyboard (also known as cell phone device, handheld device, handheld computer, palmtop or simply handheld). Examples include but are not limited to mobile computers, smart phones, cell phones, digital cameras and media players.

**Removable Media** - is any portable storage medium. Examples include but are not limited to floppy disks, jump drives, zip disks, flash cards (USB memory sticks), jaz disks, smart cards, external drives, CDs, magnetic tapes (USB, SCSI, etc.), DVDs, and PCMCIA memory cards.

**Encryption** - is the translation of data into an unintelligible condition based on a secret code. For all practical purposes, using current technology, the original data can only be restored by provision of that secret code (called Decryption).

**PROCEDURES:**

1. **Access to Electronic Protected Health Information:**
   - A. Only employees who need to use computers to accomplish work-related tasks have access to computer workstations or terminals.
   - B. All users of computer equipment are assigned an individual username and password utilizing the **Facility System Access Request Form** located on the Fundamental Resource Center. The Facility Administrator/CEO is responsible for requesting employee access to Facility network resources.
   - C. The provisioning of access to systems or applications administered by health plans or other health care providers is the responsibility of the Administrator/CEO. All User Agreements are forwarded to the Fundamental Administrative Services, LLC ("FAS") Legal Department for review.

**SUBJECT: SAFEGUARDING ELECTRONIC PROTECTED HEALTH INFORMATION (Continued)**

D. User responsibilities are outlined in the *Facility Systems User Guide*. All users execute the *Facility Systems User Guide Certification* certifying that they have been informed of and agree to comply with the responsibilities outlined in the *Facility Systems User Guide*. The *Facility Systems User Guide Certification* is available for completion on Silverchair.

E. Posting, sharing and any other disclosure of passwords and/or access codes is **not permitted** per the **Facility Information Security** standard.

F. Access to electronic protected health information is limited to employees who need the information for treatment, payment or facility operations purposes.

G. Electronic protected health information is accessed from within the Facility. Employees are permitted to access electronic protected health from outside the Facility only on an as needed basis and in compliance with the *Remote Access Policy*.

H. Employees log off the network or, at a minimum, lock their workstation when leaving the work area.

I. PHI, including an identifiable photograph, is not posted to the Internet, including social media sites (e.g. Facebook, LinkedIn, Twitter, etc.), without the express written authorization of the patient/resident or his/her legal representative. Please contact the FAS Legal Department for more information.

J. Computer monitors are positioned so that unauthorized persons cannot easily view information on the screen. Privacy filters are utilized on wall mounted devices.

K. Employee access privileges are removed promptly following the employee's separation from the Facility. The **Facility System Access Request Form** located on the Fundamental Resource Center is used to notify the FAS Information Security Department of the termination.

L. Employees immediately report any violations of this policy and procedure to their supervisor or Administrator/CEO.

2. **Storage of Electronic Protected Health Information**

A. Only Company-issued or approved hardware is used to access, store, and disclose electronic protected health information in compliance with the Hardware/Software Policy.

B. Electronic protected health information is saved/stored to network drives (i.e. M:/drive, O:/drive, etc.). Electronic protected health information is not saved/stored on the hard drive of the computer.

C. All Company-issued portable devices and removable media are password protected and encrypted where feasible in compliance with the Hardware/Software Policy.

3. **Transmission/Communication of Electronic Protected Health Information**

A. Electronic Transmissions

1) Electronic protected health information data files or datasets may only be forwarded or exchanged outside the facility network using a Secure File Transfer Facility or via a secure website. Contact the FAS Information Services Department for more information.

.

**SUBJECT: SAFEGUARDING ELECTRONIC PROTECTED HEALTH INFORMATION (Continued)**

2) Insecure methods of communication are not used to communicate electronic protected health information. This includes but is not limited to text messaging and instant messaging

B. E-mail Transmissions

1) Employees use only Company-issued e-mail accounts to communicate electronic protected health information and Facility business-related information. (firstname.lastname@fundltc.com)
2) Patient/Resident-specific information regarding highly sensitive health information shall not be sent via e-mail (i.e. information relating to AIDS/HIV, drug and alcohol abuse and psychotherapy notes).
3) Users restrict their use of e-mail for communicating normal business information such as information about operational and administrative matters, including but not limited to billing, internal auditing, quality assurance, etc. **Email is not part of the patient's/resident's medical record and is not used for treatment related purposes**.
4) All correspondence is limited to the minimum necessary to meet the needs of the recipient.
5) Electronic protected health information may be sent unprotected via e-mail within the internal network of the Company. When sending electronic protected health information outside of this network, such as over the Internet, every effort must be made to secure the confidentiality and privacy of the information. These security measures, at a minimum, include encrypting the message or the document(s) being sent. Contact the FAS Information Services Department for assistance in sending electronic protected health information outside of the network.
6) All e-mails contain a confidentiality statement (see sample below).
7) Users must exercise extreme caution when forwarding messages.
   a) Users are not to forward sensitive information, including patient/resident information, to any party outside the organization without using the same security safeguards as specified above.
   b) Users shall not forward electronic protected health information without proper patient/resident authorization when required.
8) Users may periodically delete e-mail messages that are no longer needed for business purposes, per the Company's Document Management policy.
9) Employee e-mail access privileges are removed promptly following their separation.
10) E-mail messages, regardless of content, are not considered secure or private. Limit the amount of information, in any e-mail, to the minimum necessary to meet the needs of the recipient.

**SUBJECT: SAFEGUARDING ELECTRONIC PROTECTED HEALTH INFORMATION (Continued)**

Sample Confidentiality Statement

The information contained in this e-mail is legally privileged and confidential information intended only for the use of the individual or entity to whom it is addressed. If the reader of this message is not the intended recipient, you are hereby notified that any viewing, dissemination, distribution, or copying of this e-mail message is strictly prohibited. If you have received and/or are viewing this e-mail in error, please immediately notify the sender by reply e-mail, and delete this e-mail from your system. Thank you.

**Destruction of Electronic Protected Health Information:**

A. Electronic Hardware and Media: Prior to the disposal of any electronic hardware or media, including donation, sale or destruction, all electronic protected health information is permanently removed from the equipment. Contact the FAS Information Services Department regarding disposal. Follow EPA Guidelines regarding disposal of computer equipment.

B. Backup or Data Tapes: Rotate tapes and recycle them until they are no longer useable. Prior to disposal, electronic protected health information is permanently removed. Contact the FAS Information Services Department regarding disposal.

5. Employees should immediately report any violations of this policy or potential breach of patient/resident information to their supervisor or Administrator/ CEO.

**REFERENCES:**

1. **HIPAA Final Privacy Regulations**; 45 CFR § 164.530

## SUBJECT: SAFEGUARDS - POSTED PROTECTED HEALTH INFORMATION

### POLICY:

Protected Health Information (PHI) is not be used or disclosed in a manner that violates the HIPAA Privacy Rule, Facility's Policies and Procedures or any other federal or state regulation governing confidentiality and the privacy of health information. The staff prevents the prohibited uses and disclosures of PHI and limits incidental uses and disclosures when PHI is posted within the Facility for permitted purposes. PHI is not posted or displayed in a public location except as allowed by the HIPAA Privacy Rule and identified in the *Notice of Privacy Practices* or as required by federal and state laws and regulations.

### PROCEDURES:

1. Use or disclosure of PHI is limited to that which is described in the *Notice of Privacy Practices*.

2. Posted PHI is intended for viewing only by staff involved in patient/resident care and is not displayed in a place or manner which is easily accessible to unauthorized persons. This includes common areas such as individual offices and staff break-rooms where family, visitors, staff members without PHI access, volunteers and/or other patients/residents might view the information.

3. The Facility obtains approval from the Fundamental Administrative Services, LLC ("FAS") Legal Department for all other uses or disclosures patients'/residents' PHI. If the use or disclosure is approved, the FAS Legal Department provides appropriate authorizations and releases to be signed by the patient/resident or legal representative. Approval is also required prior to posting patient/resident information or photographs to the Internet, including social networking websites, i.e. Facebook, Twitter, LinkedIn, etc.

### REFERENCES:

1. **HIPAA Final Privacy Regulations**
   45 CFR § 164.530

## SUBJECT: PRIVACY OF PATIENT/RESIDENT PHOTOGRAPHIC IMAGES

### POLICY:

It is the Facility's policy to protect its patients/residents, within reasonable limits, from invasion of privacy that might occur from the use of patient/resident photography, videotaping, digital imaging, and other visual recordings during treatment or other Facility activities. The Facility must obtain specific written consent from the patient/resident prior to photographing and/or disclosing the patient/resident photography. It is strictly prohibited to photograph patients/residents without obtaining their prior written consent.

### DEFINITIONS:

**Patient/Resident Photography** means the likeness of a patient/resident that may be recorded through a number of visual means, including still photography, videotaping, digital imaging, scans, and others. Throughout this policy, the term "patient/resident photography" will be used for any such recording of a patient/resident's likeness.

**Protected Health Information (PHI)** is defined as individually identifiable health information that is maintained or transmitted by a healthcare provider in any form, including electronic records, paper records and oral discussions. Some examples of protected health information are interdisciplinary progress notes, physician's orders, care plans and billing information that contains patient/resident health information.

**Marketing** is a communication about a product or service that encourages recipients of the communication to buy or use the product or service. Marketing specifically includes arrangements between the Facility and another party, whereby the Facility discloses PHI to the other party in exchange for direct or indirect compensation, so that the third party or its affiliate can make a communication about its own product or service that encourages the patient/resident to buy or purchase that product or service.

Marketing does not include communications by the Facility to the patient/resident:

1. For treatment purposes; or
2. For case management or care coordination; or
3. To recommend alternative treatments, therapies, health care providers or setting of care.

**Treatment** is the provision, coordination, or management of health care and related services by the Facility, including the coordination or management of health care by the Facility with a third party; consultation with other health care providers relating to a patient/resident; or the referral of a patient/resident for health care between the Facility and another health care provider.

**Health Care Operations** is any of the following activities of the Facility:

1. Conducting quality assessment and improvement activities, provided that the obtaining of general knowledge is not the primary purpose of any studies resulting from such activities; protocol development, case management and care coordination, contacting health care providers and patients/residents with information about treatment alternatives; and related functions that do not include treatment;

**SUBJECT: PRIVACY OF PATIENT/RESIDENT PHOTOGRAPHIC IMAGES (Continued)**

2. Reviewing the competence or qualifications of health care professionals, evaluating employee and Facility performance, conducting training programs under supervision to practice or improve skills, training non-health care professionals, accreditation, certification, licensing, or credentialing activities;

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

4. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the Facility;

5. Business management and general administrative activities of the Facility, including, but not limited to:
   A. Customer service;
   B. Resolution of internal grievances;
   C. Due diligence in connection with the sale or transfer of assets to a potential successor in interest;
   D. Creating de-identified health information and marketing for which a patient's/resident's authorization is not required.

**PROCEDURES:**

**CONSENTS AND AUTHORIZATIONS**

**Consent to Photograph for Treatment Related Purposes**

1. The Facility must obtain specific written consent from the patient/resident or legal representative prior to photographing for all purposes except in cases of:
   A. Abuse;
   B. Neglect;
   C. Emergencies; and
   D. Photography obtained for personal/family use (e.g. photographs used for family photo albums, or other private use).

2. The Facility must obtain specific written consent to photograph for treatment.
   A. Photographs for treatment purpose are used for patient/resident identification, infection control, surveillance; and/or other medical purposes.

**Consent to Photograph and Authorization to Release Photography for Recreational Purposes**

The Facility will ensure that all patients/residents or their legal representatives give specific written permission prior to using/disclosing a patient's/resident's name, photograph, or other likeness for purposes other than treatment or continuation of care.

**SUBJECT: PRIVACY OF PATIENT/RESIDENT PHOTOGRAPHIC IMAGES (Continued)**

**Consent to Photograph and Authorization to Release Photography for Marketing Purposes**

1. In accordance with the Facility's Marketing Policy for the use and/or disclosure of PHI for marketing purposes, the Facility must obtain the patient/resident or his/her legal representative's written authorization prior to taking or disclosing a patient/resident photograph in conjunction with a marketing communication.

2. Consult Fundamental Administrative Services, LLC (FAS) Legal Department before instituting new marketing programs that involve patients/residents. The FAS Legal Department will provide the proper authorizations and releases for the marketing program. (Refer to: *Marketing Policy* in this section.)

**PATIENT PHOTOGRAPHY**

**Taking of Photographic Images**

1. Only take photographs using Facility approved digital equipment purchased through the DSSI Purchasing System on the Fundamental Resource Center (FRC). Employees **do not** use their own photographic equipment to take photographs of patients/residents; this includes personal cell/smart phones with cameras.

2. The patient's/resident's dignity and modesty are considered at all times. Only photograph the minimum required area of the body.

**Printing of Photographic Images**

Only print photographs using Facility approved equipment. Employees **do not** use their own equipment to print photographs. **Do not** use third party vendors such as Snapfish, Kodak, Shutterfly, Ritz, Walgreens, etc. to print patient/resident photographs.

**Disclosure of Photographic Images**

Only photographs specifically authorized through a written authorization may be released to authorized persons. Patient/resident photographs will not be posted to the Internet, including social media sites (e.g. Facebook, LinkedIn, Twitter, etc.), or sent through email without the patient's/resident's specific written authorization. Please contact the FAS Legal Department for more information.

**Storing of Photographic Images**

1. Facility must appropriately identify photographs with patient/resident name, medical record number, and date of admission.

2. Photographs which form part of the medical record should be securely fixed to the record and in chronological order.

**SUBJECT: PRIVACY OF PATIENT/RESIDENT PHOTOGRAPHIC IMAGES (Continued)**

3. Photographs taken in relation to an accident or incident should be securely attached to the Incident Report Form.

4. Facility must permanently delete digital images recorded through a camera or PC immediately after the image has been printed. (Contact the FAS Support Center for assistance.)
   A. If a digital image needs to be retained electronically, this should be made explicit in the consent/authorization process. In addition, the digital image must be retained on a secure network drive. The digital image is permanently deleted after the required retention period has expired in accordance with the *Document Management Policy*.

5. For images stored in a clinical or financial application, consult the applicable system's user guide for storage instructions.

6. Security and confidentiality requirements for other paper or electronic health records also apply to photographic images.

## SUBJECT: HIPAA DOCUMENTATION

## POLICY:

The Privacy Designee or his/her designee will document the following types of activities related to compliance with the requirements the Privacy Rule on the HIPAA Request and Response Log. This log and supporting documentation will be maintained in the patient's/resident's medical record for a period of no less than six (6) years from the date it was created:

1. Requests for:
   - A. Restrictions
   - B. Alternate Communication
   - C. Amendment
   - D. Accounting of Disclosure

The Privacy Designee or his/her designee will document requests for disclosure/release of medical records on the HIPAA Correspondence Log. This log and supporting documentation will be maintained for a period of no less than six years from the date it was created.

## PROCEDURES:

HIPAA Request and Response Log

1. The Privacy Designee or his/her designee creates a record in the **HIPAA Request and Response Log** upon the occurrence of each of the following HIPAA activities:
   - A. Requests for:
     - 1) Restrictions
     - 2) Alternate Communication
     - 3) Amendment
     - 4) Accounting of Disclosure
2. All supporting request/response forms and documentation are kept behind the **HIPAA Request and Response Log** under the "**HIPAA"** tab in the patient's/resident's medical record.
3. The **HIPAA Request and Response Log** and supporting documentation are maintained for a period of no less than six (6) years from the date of creation.
4. The Privacy Designee or his/her designee is responsible for keeping the **HIPAA Request and Response Log** current, and entering the required information as soon as possible after the request or activity takes place.
5. The Privacy Designee or his/her designee enters the patient/resident information (name and medical record number) and facility name and number in the header information.
6. The Privacy Designee or his/her designee enters the information relevant to the particular request or activity.

**SUBJECT: HIPAA DOCUMENTATION (Continued)**

**1. The following outlines the information required for completion of the HIPAA Request and Response Log:**

A. Date of Request
   1) Date Completed Request was Received

B. Type of Request
   1) Restriction
   2) Alternate Communication
   3) Amendment
   4) Accounting

C. Requestor
   1) Patient/Resident or
   2) Legal Representative

D. Time Extension Requested
   1) Yes, No, N/A

E. Request Granted
   1) Yes or No

F. Date Request Completed
   1) Date Resident Notified of Response
   2) Date Provided Requested Information
   3) Date Other Entities Notified of Amendment (if applicable)

HIPAA Correspondence Log

1. The Privacy Designee or his/her designee creates a record on the **HIPAA Correspondence Log** upon the occurrence of each request for disclosure/release of medical records. The **HIPAA Correspondence Log** can either be (depending on volume):
   A. A log dedicated to one patient's/resident's disclosures, or
   B. A log containing multiple patients/resident disclosures.

2. All original disclosure/release documentation (i.e. Authorization & Request for Release of Medical Records, Subpoenas, Court Orders, Ombudsman Access to Records) is kept with the **HIPAA Correspondence Log** in a HIPAA binder or folder.

3. The **HIPAA Correspondence Log** and supporting documentation are maintained for a period of no less than six (6) years from the date of creation.

4. The Privacy Designee or his/her designee is responsible for keeping the **HIPAA Correspondence Log** current, and entering the required information as soon as possible after the request takes place.

5. The Privacy Designee or his/her designee enters the patient/resident information (name and medical record number).

**SUBJECT: HIPAA DOCUMENTATION (Continued)**

6. The Privacy Designee or his/her designee enters the information relevant to the particular request or activity.

**7. The following outlines the information required for completion of the HIPAA Correspondence Log:**

A. Date of Request - Date Request was Received
B. Requestor
C. Approved by Legal Department -Yes or No
D. Request Granted - Yes or No
E. Date of Disclosure
F. HIPAA Compliant Authorization - Yes or No

**REFERENCES:**

**1. HIPAA Final Privacy Regulations**
45 CFR § 164.530

**HIPAA PRIVACY AND MEDICAL RECORD POLICIES & PROCEDURES**

## HIPAA Request and Response Log

Patient's/Resident's Name: _____

Medical Record Number: _____

Facility's Name: _____

| Date of Request | Type of Request | Requestor | Response to Request | Date Request Completed |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

**HIPAA PRIVACY AND MEDICAL RECORD**
**POLICIES & PROCEDURES**

## HIPAA Correspondence Log

Facility's Name:
_____

| Patient/ Resident | Medical Record # | Date of Request | Requestor | Approved by Legal (Y/N) | Request Granted (Y/N) | Date of Disclosure | HIPAA Compliant Authorization (Y/N) |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

## SUBJECT: HIPAA TRAINING

### POLICY:

Facility employees receive privacy and security related training in a timely manner and appropriate to the employee's job responsibilities. The Privacy Designee or his/her designee is responsible for verifying that employees receive assigned training in a timely manner.

Training materials and proof of training are maintained for a period of no less than six years from the date the training is provided. Consultants, contractors, volunteers, temporary staff, interns and students may be required to receive privacy and security related training as deemed appropriate.

### PROCEDURES:

The following trainings are provided to employees and appropriate individuals as specified:

HIPAA Level I Privacy Training

| | |
|---|---|
| **Content Description** | Intro to HIPAA Privacy and Security DVD with written materials |
| **Trainees** | -All facility employees |
| **Delivery Method** | -DVD - Operation HIPAA: For Your Eyes Only<br>order from InnerWorkings<br>-Track participation in Fundamental University (Silverchair Learning Systems) |
| **Frequency** | -Upon Orientation – within 30 days of hire<br>-Annually – January |

HIPAA Level II Privacy Training

| | |
|---|---|
| **Content Description** | In-depth information on HIPAA Privacy with case studies |
| **Trainees** | -License clinical staff<br>-Business office<br>-Admission<br>-Social Work<br>-Activities |
| **Delivery Method** | -Fundamental University (Silverchair Learning Systems) |
| **Frequency** | -Upon Orientation – within 30 days of hire<br>-Annually – August |

HIPAA Level III Privacy Training

| | |
|---|---|
| **Content Description** | In-depth information on HIPAA Privacy and Security requirements with policy references |
| **Trainees** | -Medical Records Staff<br>-Privacy Designee<br>-Administrator or equivalent position |
| **Delivery Method** | -Fundamental University (Silverchair Learning Systems) |
| **Frequency** | -Upon Orientation – within 30 days of hire<br>-Annually – December |

Safeguarding Electronic Protected Health Information

| | |
|---|---|
| **Content Description** | Safeguarding Electronic Protected Health Information Policy with examples and a System User Certification |
| **Trainees** | All facility employees |
| **Delivery Method** | -Fundamental University (Silverchair Learning Systems) |
| **Frequency** | -Upon Orientation – within 30 days of hire<br>-Annually – October |

Business Associate Policy

| | |
|---|---|
| **Content Description** | Business Associate Policy |
| **Trainees** | Administrator or equivalent position |
| **Delivery Method** | -Fundamental University (Silverchair Learning Systems) |
| **Frequency** | -Upon Orientation – within 30 days of hire |

Breach Notification Policy

| | |
|---|---|
| **Content Description** | Breach Notification Policy |
| **Trainees** | Administrator or equivalent position |
| **Delivery Method** | -Fundamental University (Silverchair Learning Systems) |
| **Frequency** | -Upon Orientation – within 30 days of hire |

| | |
|---|---|

Access Request Policy

| | |
|---|---|
| **Content Description** | Access Request Policy |
| **Trainees** | -Administrator or equivalent position<br>-Business Office Manager<br>-Director of Nursing or equivalent position |
| **Delivery Method** | -Fundamental University (Silverchair Learning Systems) |
| **Frequency** | -Upon Orientation – within 30 days of hire |

**REFERENCES:**

1. **HIPAA Final Privacy Regulations**
   45 CFR § 164.530

## SUBJECT: DEFINITION OF INDIVIDUAL SIGNING AUTHORIZATION

## POLICY:

Designated individuals will sign authorization forms, when applicable.

## PROCEDURES:

Following are definitions of individuals who may sign authorizations:

1. Patient/Resident: A patient/resident who is a competent adult may sign a release form. The Facility assumes competency unless there is documentation that the patient/resident was adjudicated incompetent by a court of law or declared incapable in writing by an examining physician or by two examining physicians if required by state law. If the patient's/resident's condition raises questions about his/her competency and there is no written determination that declares the patient/resident incompetent or lacking capacity to make decisions, the Facility shall have the patient/resident evaluated by a physician to make a determination, in accordance with state law, whether the patient/resident is capable of making his/her own decisions.

   A patient/resident who is a minor may authorize the release of information concerning treatment to which he could consent under applicable law.

2. Patient's/Resident's legal representative: If the patient/resident is a minor or is incompetent, the release form is signed by his/her legal representative.
   A. In the case of a minor this would include a parent, probate conservator, guardian or any other person who has lawful custody.
   B. In the case of incompetent adult patients/residents, either a probate guardian/conservator of the patient's/resident's person or psychiatric guardian/conservator of the patient's/resident's person authorizes disclosure as the patient's/resident's legal representative.

3. Patient's/Resident's spouse: If the patient/resident is incompetent and has no designated legal representative, the spouse of the patient/resident or person financially responsible for the patient/resident signs the release form for the limited purpose of processing an application for health insurance or for enrolling the patient/resident in a health insurance plan where the patient/resident is to be an enrolled spouse or dependent under the policy or plan.

4. Patient's/Resident's personal representative: Information regarding a deceased patient/resident is released upon the signature of an individual who has been declared the executor or the administrator of the patient's/resident's estate. Court documentation regarding the identity of the executor must be received prior to release.

**SUBJECT: RECEIPT OF A SUBPOENA DUCES TECUM (MAY ALSO BE REFERRED TO AS A SUBPOENA DUCES TECUM)**

**POLICY:**
The Administrator or Custodian of Medical Records will be empowered to accept a subpoena directed to the Custodian of Medical Records at the facility.

**PROCEDURES:**

1. Subpoenas can be served by mail, a private process server, or Sheriff.

2. A subpoena may be addressed to the Administrator or Custodian of Medical Records and should reference the Facility to which it is addressed.

3. If a subpoena is being served in person, before accepting, verify that the subpoena has been delivered to the correct Facility. The Administrator or Medical Records personnel should be notified to accept service on behalf of the Facility.

4. If the subpoena does not identify the Facility sufficiently, you may tell the process server that they have not served the proper Facility and you may refuse service.

5. Write the date and time and method of receipt (i.e., certified mail, private process, etc.) on the subpoena.

6. Immediately forward a copy of the subpoena to the Fundamental Administrative Services, LLC (FAS) Legal Department pursuant to the *Disclosure of Protected Health Information (PHI)/Medical Records* policy. Identify if the medical record being requested contains records of a psychiatric nature, drug or alcohol abuse or HIV or AIDS history. (See *Receipt of A Subpoena for Medical Records Which May Contain Records of Psychiatric Nature Drug or Alcohol Abuse or HIV or AIDS History* policy.)

   NOTE: If the subpoena is for employee records, forward subpoena to the Human Resources Coordinator at the Facility for forwarding to the FAS Legal Department.

7. Search the Master Patient/Resident Index to locate the patient/resident's record. Retrieve from the record storage if necessary.

8. Make note of the date of the scheduled deposition or court appearance, or date by which the records must be retrieved if they may be mailed. Follow-up with FAS Legal Department if the date is approaching and you have not received a reply. If you determine additional time is needed so that a record can be retrieved from storage or you need additional time for copying, contact the requesting attorney/records retrieval company to request additional time to comply. If the requesting party is not cooperative, contact FAS Legal Department for assistance.

9. Wait for further instructions from FAS Legal Department prior to disclosing any information.

**SUBJECT: RECEIPT OF A SUBPOENA DUCES TECUM (MAY ALSO BE REFERRED TO AS A SUBPOENA DUCES TECUM) (Continued)**

**PREPARATION OF RECORDS:**

1. If billing statements are also requested, notify the Business Office.

2. Remove all correspondence, release of information authorizations, other subpoenas and any other documents if these documents are not covered by the description of documents being subpoenaed.

3. Copy the records, checking each page of the copy to determine if the copies are legible.

4. Stamp each page of the copy with the re-disclosure and confidentiality penalty statement or similar stamp to ensure the confidentiality of records is followed.

5. Complete an **Affidavit of Custodian of Medical/Billing Records** and sign. Follow the instructions on the subpoena for mailing the documents to the requesting party. Mail by registered mail with a return receipt requested.

6. Place a copy of the subpoena and affidavit in the **HIPAA Correspondence Log** and with the original medical record.

**PROCEDURES WHEN ORIGINAL RECORD IS TO BE TAKEN TO COURT BY CUSTODIAN OF RECORDS:**

1. The custodian of records retains the witness fee check.

2. The copy is prepared as noted above and double enveloped.

3. The original record and copy is taken to the court proceeding. The original record is not left with the Court unless ordered by the presiding judge.

4. In the event that the original is ordered to be left with the Court, the copy is returned to the Facility.

5. Request a receipt for the original record from the court bailiff. The Facility should retain a copy of the record along with the receipt from the Court.

## AFFIDAVIT OF CUSTODIAN OF MEDICAL/BILLING RECORDS

**ON BEHALF OF _____**

STATE OF _____ )
) ss:
COUNTY OF _____ )

I, _____, being first duly sworn, state the following:
CUSTODIAN OF RECORDS

1. That the Affiant is the Custodian of Records for

_____ and in such capacity, is the custodian of any and all medical records, diagnostic images of any kind, (x-ray films, MRIs, CT scans, etc.), diagnostic imaging reports, laboratory reports, results, prescriptions and other records and/or billing statements of the office.

2. That Affiant was served with an AUTHORIZATION AND/OR SUBPOENA to release any and all medical and/or psychiatric records, diagnostic images of any kind, (x-ray films, MRIs, CT scans, etc.), diagnostic imaging reports, laboratory reports, results, prescriptions and other records and/or billing statements requesting the production of any and all medical and/or psychiatric records, diagnostic images, diagnostic imaging reports, laboratory reports, results, prescriptions and other records and/or billing statements pertaining to _____(Patient/Resident) for the period of all treatment to the present date.

3. That the Deponent has examined the original of those records and has made a true and exact reproduction copy of them.

4. That the original of those records, diagnostic images, diagnostic imaging reports, laboratory reports, results, prescriptions and other records and/or billing statements was made at or near the time of the acts, events, conditions, opinions, or diagnosis recited therein by or from information transmitted by a person with knowledge in the course of a regularly conducted activity of the deponent or the office or institution in which the deponent is engaged.

DATED this _____ day of _____, _____.

_____
CUSTODIAN OF RECORDS

Print Name: _____

SUBSCRIBED and sworn to before me
this ___ day of _____, _____.

## SUBJECT: REDISCLOSURE OF PRIVILEGED INFORMATION

**POLICY:**
The Administrator or Custodian of Medical Records will verify that medical, rehabilitation, psychiatric, drug and alcohol abuse information released to the Facility by another facility or physician, but maintained in the facility's medical record of adjunct records, will not be released by the facility.

**PROCEDURES:**

1. Medical information brought to the Facility by the patient/resident, parent or legal representative for purposes of Continuity of Care is maintained by the facility.

2. Information identified in Item 1 above is returned to the individual who originally brought the information to the facility at the time of patient/resident discharge or upon request.

3. The information received from another facility that is used for the diagnostics or treatment of a patient/resident, becomes part of the medical record.

4. Information that has been released to the facility by authorization of the patient/resident, the parent of the patient/resident, or the legal representative from a third party is not released a second time by the facility unless it is to the patient/resident or legal representative to whom the information applies with the following disclaimer.

    a. "The medical records covering dates of service for _____ (patient's/resident's name) from _____ to _____ were created by _____ (hospital or physician's name). This facility cannot certify as to their content, completion, trueness or accuracy. It is, therefore, recommended that you contact _____ for a complete copy of these documents."

5. After discharge, the records from another facility or physician are maintained in the back of the record. The disclaimer, which follows, is filed in the medical record preceding information from other facilities/providers.

6. Refer to "Sample Language for Confidentiality Stamp."

Sample Language for Confidentiality Stamp.

* * * * * * * * * * * * * * * * * *

**THIS INFORMATION IS OF A**

**HIGHLY CONFIDENTIAL NATURE,**

**IS PROTECTED BY**

**FEDERAL AND STATE STATUTES**

**AND UNDER NO CIRCUMSTANCES IS**

**TO BE RELEASED TO**

**ANOTHER PARTY.**

* * * * * * * * * * * * * * * * * *

**SUBJECT:** **RECEIPT OF A SUBPOENA FOR MEDICAL RECORDS WHICH MAY CONTAIN RECORDS OF A PSYCHIATRIC NATURE, DRUG OR ALCOHOL ABUSE OR HIV OR AIDS HISTORY.**

**POLICY:**
Records will only be released pursuant to applicable state and federal law, and procedures as set out in the subpoena.

**PROCEDURES:**

1. The subpoena is received and forwarded to the Fundamental Administrative Services, LLC (FAS) Legal Department for review. Identify for the FAS Legal Department that the medical record contains records of a psychiatric nature, drug or alcohol abuse or HIV or AIDS history.

2. Wait for instructions from the FAS Legal Department regarding disclosure of this information

## SUBJECT: FACSIMILE TRANSMISSIONS

### POLICY:

Facsimile transmission of patient/resident protected health information will be carried out in a manner that promotes confidential, quality, cost effective care and service.

### PROCEDURES:

1. Plain paper facsimile equipment is used when possible. In situations in which thermal process machines are utilized:
   - A. Copies of thermal bond transmissions are made onto plain paper, bond quality material.
   - B Thermal bond transmissions are immediately destroyed by shredding.

2. Upon receipt of a facsimile transmission, the person performing the intake:
   - A Verifies patient/resident identification to be certain that all documents received are intended for receipt.
   - B Verifies that the number of pages is consistent with the total number stated on the cover transmission sheet.
   - C Contacts the sender if pages are missing or unreadable.
   - D Routes the material to the intended recipient as indicated, or files it in the patient/resident medical record.

3. Faxing protected health information is limited to circumstances where the information is needed immediately and more secure transmission methods are not feasible. For example, protected health information may be transmitted via facsimile when urgently needed for patient/resident care or required by a third-party payer for ongoing certification of payment for a patient/resident.

4. Protected health information transmitted must be limited to the minimum necessary to meet the requester's needs.

5. Except as authorized by federal or state law, the patient's/resident's or legal representative's written authorization must be obtained prior to releasing protected health information in compliance with the *Disclosure of Protected Health Information (PHI)/Medical Records* policy.

6. The following types of medical information are protected by federal and/or state statute and may NOT be faxed unless required by law.
   - A Sexually transmitted disease cases, including HIV and AIDS
   - B Drug or substance abuse cases
   - C Psychiatric, mental health or behavioral management cases

7. The receipt of information for a patient/resident referral via facsimile transmission does not constitute acceptance of the patient/resident to the facility's services.

**SUBJECT: FACSIMILE TRANSMISSIONS (Continued)**

8. Prior to transmitting any information via facsimile, the sender:
   A. Prepares a transmittal cover sheet, which includes:
      1) Name, telephone number and fax number of sender;
      2) Name, telephone number and fax number of intended recipient; and
      3) A confidentiality notice substantially in the following form:
         a) *"The information in this transmittal is intended for the individual or entity named above. It is legally privileged and confidential. If you have received this information in error, notify us immediately by calling the number set below. Send the original transmission by mail. Return postage is guaranteed. If the reader of this message is not the intended recipient, you are hereby notified that any disclosure, dissemination, distribution or copying of this communication or its contents is strictly prohibited."*
   B. Keys in the facsimile telephone number of the intended recipient.
   C. Verifies the facsimile telephone number entered on the equipment keypad or speed dial list.

9. Following a transmission, the sender:
   A. Retains the transmittal sheet.
   B. Places the transmittal cover sheet, transmitted document, and fax confirmation sheet in an organized tracking system (i.e. log/file).
   C. The transmitted document is to be filed in the medical record with the following information:
      1) Date, time, and person's name sending the document
      2) Date, time, and person's name receiving the confirmation sheet
         a) This could be validated by cross-checking with the tracking system.
         b) When the patient/resident is discharged from care, the validation information is placed in the discharge chart.

**Misdirected Faxes:**

10. If a fax transmission containing protected health information is not received by the intended recipient because of a misdial, check the internal logging system of the fax machine or the fax confirmation sheet to obtain the misdialed number.

11. If possible, a phone call (supplemented by a note referencing the conversation) should be made to the recipient of the misdirected fax requesting that the entire content of the misdirected fax be destroyed. If the recipient cannot be reached by phone, a notification including the fax confirmation sheet should be faxed to the recipient requesting that the entire content of the misdirected fax be destroyed.

12. Misdirected faxes may constitute a breach of protected health information therefore the Administrator is notified immediately.

**SUBJECT: RECORD PROTECTION FROM DAMAGE**

**POLICY:**
Precautions are taken for the safekeeping, protection against loss, defacement, tampering and use by unauthorized individuals of the medical records.

**PROCEDURES:**

1. Record Control (refer to specific policies and procedures in Section V).

2. No smoking policy is in effect within the Facility.

3. Liquids in uncovered containers are not permitted on employee desks when working with charts.

4. In the event of flood or hurricane or other natural disasters, records are removed from the two lowest shelves, boxed and placed on top shelves or on desk tops.

5. Medical Records are kept in a locked cabinet or office when unattended or when the Facility is closed.

6. When records/data are destroyed inadvertently (such as fire or flood) notification shall be made as follows:
   A. Internal notification of Administration. For records that meet minimum regulatory requirements but not organizational requirements, the certificate of destruction shall carry the information relating to the inadvertent destruction.
   B. External notification of licensure/regulatory and accrediting agencies if applicable. For records that do not meet minimum regulatory or accrediting agency timeframes the Administrator makes notification. The notice to the Administrator includes the information relating to the cause of the inadvertent destruction.
   C. All inadvertent and malicious destruction of records/data are reported to Fundamental Administrative Services, LLC (FAS) Legal Department and the FAS Privacy Officer.

**SUBJECT:** **INFORMATION MANAGEMENT RETENTION**

**POLICY:**
The Medical Record is retained for the period required by state laws.

**PROCEDURES:**

1. Medical Records staff are responsible for maintaining all medical records according to all state, federal and Facility policy and procedure.

2. Medical Records staff provide assistance to all other departments in developing retention schedules for their records, data, indexes, and reports.

3. The following schedule is followed for all documents
   - A. Medical record
     - 1) Refer to Documentation Management policy for retention periods.
   - B. Master patient index
     - 1) Permanent
   - C. Admission/Discharge Register
     - 1) Permanent

**SUBJECT:** **LONG TERM STORAGE OF RECORDS**

**POLICY:**

Precautions are taken for the safekeeping, protection against loss, defacement, tampering and access by unauthorized individuals of records while in storage. Records stored off premises are accorded the same security, protection from theft, and preservation that they would have if they were retained in the Facility. Records in storage are maintained in an organized manner in order to provide for timely access and retrieval.

**PROCEDURES:**

1. All Facility records placed in long term storage are recorded and are protected against loss, defacement, tampering and access by unauthorized individuals

Medical Record Storage:

2. On at least an annual basis records for the previous year are placed into long term storage.

3. Medical records to be stored are organized by date of discharge in order to provide for timely access and retrieval.

4. The patient's/resident's name, medical record number, dates of service and date of birth are recorded on the Medical Records Storage Log prior to placing the medical record into storage.

5. If a document storage vendor is used for offsite storage, maintain the storage receipt with the Medical Records Storage Log.

## MEDICAL RECORDS STORAGE LOG

| Patient/Resident Name | Medical Record Number | Dates of Service | Date of Birth | Box Number |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## SUBJECT: INFORMATION MANAGEMENT DESTRUCTION

**POLICY:**
Patient/Resident medical records are destroyed upon the expiration of state regulatory retention periods, with the exception of records maintained for patients/resident for whom there may be pending litigation. Refer to the *Document Management Policy*.

**PROCEDURES:**

1. The Medical Record Storage Log is reviewed page by page to determine the age of all charts stored in particular boxes and charts which may belong to a minor.

2. Stored charts which have a discharge date older then the retention period mandated by state law are identified. Refer to the *Document Management Policy* for retention periods.

3. Any chart belonging to a minor or where there may be pending litigation is retrieved from the boxes scheduled for destruction and returned to storage facility. The charts are logged and packed in new boxes and returned to storage

4. The destruction process is discussed with the Facility Administrator.

5. When all interested parties have been notified of the intended destruction, the storage facility is requested to destroy the records filed in specific boxes.

6. Complete a list of records to be destroyed:
   A. Patient/Resident name
   B. Medical Record Number
   C. Admission Date
   D. Discharge Date

7. Records containing patient/resident identifiable data are destroyed in a manner that makes it impossible to reconstruct and read the information.

8. Acceptable methods of destruction are shredding, incineration, and pulverization.

9. If Facility staff is responsible for destroying the information, health information management staff is present during the process.

10. If medical records are destroyed off-site through a destruction company, a certificate attesting to the destruction of the medical records is obtained.

11. The Record Destruction Certificate is filed with the Medical Record Destruction Log.

**HIPAA PRIVACY AND MEDICAL RECORD POLICIES & PROCEDURES**

## MEDICAL RECORD DESTRUCTION LOG (Individual Patient/Resident Records)

| PATIENT/RESIDENT NAME | MEDICAL RECORD NUMBER | ADMISSION DATE | DISCHARGE DATE |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Date of Destruction:_____ Destroyed by:_____

Witness: _____

## SUBJECT: RETRIEVAL OF A MEDICAL RECORD FROM STORAGE FACILITY

## POLICY:

All records in storage will be provided to the requester in compliance with federal and state laws and regulations.

## PROCEDURES:

1. Medical records receive a request for a record.

2. The Master Patient Index is reviewed to determine the medical record number and the admission and discharge dates.

3. If the record is beyond a certain age, it may have been sent to storage.

4. Review the Medical Record Storage Log for patient/resident.

5. Determine if the record you require is in storage.

6. If the record is in storage, call the document storage facility, if applicable, and provide the following information:
   A. Box number
   B. Patient/Resident name
   C. Patient/resident medical record number
   D. If the record is to be delivered within 24 hours, indicate this information to the storage facility personnel.
   E. If the record is to be delivered STAT, indicate this information to the storage facility personnel.

7. When the record is delivered, notify the department or physician requester that the record is available if applicable.

8. Maintain the delivery receipt with the Medical Record Storage Log.

9. Use the delivery receipt to verify accuracy of billing.

10. When the requester has returned the record in question or the record has been copied pursuant to a request for release of information, pack in a box for storage pickup.

11. Do not return one chart at a time. Return several charts at a time.

**SUBJECT: MAINTENANCE OF THE MASTER PATIENT INDEX**

**POLICY:**
All patients/residents admitted will have a Master Patient Index entry or card filed in the Master Patient Index.

**PROCEDURES:**

1. The Facility maintains the Master Patient Index entry for all patients/residents admitted.

2. Master Patient Index contains the following information at a minimum:
   a. First, middle and last name of patient/resident
   b. Date of Birth
   c. Facility medical record or patient/resident number
   b. Admission dates
   c. Discharge dates and discharge dispositions

3. The Master Patient Index may be maintained electronically in a clinical system.

**NOTE**:

The Master Patient Index remains as a permanent record of all patients/residents who have been admitted to the Facility.

## SUBJECT: MAINTAINING RECORD CONTROL

## POLICY:

The Facility maintains a medical record that documents care and services provided to the patient/resident. In addition to its clinical purposes, the medical record is the legal business record for the Facility and is maintained in a manner that complies with applicable regulations, accreditation standards, professional practice standards, and legal standards. The custodian of the legal business record, establishes and maintains all patient's/resident's filing and record use and is responsible for maintaining the integrity of and preventing unauthorized access to a patient's/resident's medical record.

## PROCEDURES:

1. Original records are not removed from the Facility. For more information, contact the Fundamental Administrative Services, LLC Legal Department.

2. In order to provide proper medical record control, all medical records taken from Medical Records are signed out.

3. The Medical Record Sign Out Log is located in Medical Records, and the following information is recorded on the log: patient/resident name, date of removal, patient/resident medical record number, name of the requestor, location to which the chart is being taken, and expected return date.

4. Outguides provide an important means of control over record usage. They are used as a placeholder for a record that has been removed from the files. The Outguide is to remain in the file until the signed out chart is returned and refiled.

**HIPAA PRIVACY AND MEDICAL RECORD**
**POLICIES & PROCEDURES**

**MEDICAL RECORD SIGN-OUT SHEET**

| TODAY'S | | PATIENT/ RESIDENT NAME | MEDICAL RECORD NUMBER | TAKEN BY | LOCATION | EXPECTED DATE OF RETURN | DATE OF RETURN |
|---|---|---|---|---|---|---|---|
| DATE | TIME | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

## SUBJECT: CHART ORDER AND THINNING

## POLICY:

All charts are assembled in a standardized manner to provide that all documentation is accurate and appropriate. In-house charts will be thinned on an as needed basis. Records removed from the chart will be taken to Medical Records or protection until discharge.

## PROCEDURES:

1. The thinned records are organized in the same order as the discharged record order. All like forms are filed together in date order.

2. All overflow records are removed from the active record and filed in the patient's/resident's permanent folder in Medical Records.

3. Any records that appear to be missing are identified and the applicable individuals are notified that their records appear to be deficient. They are asked to provide the records immediately.

4. This thinning process assists Medical Records in maintaining control of the record on a concurrent, as well as a discharge basis.

**SUBJECT: CHART ORDER AND THINNING (Continued)**

## RECOMMENDED CHART ORDER

**Admission Documentation**
DNR/CPR Directive (recommend plastic sleeve)
Admission Record/Facesheet
Advance Directive
Preadmission Assessment/Intake
Admission Consent Permanent
Admission Agreement

**Physicians Orders**

**History & Physical and Hospital Transfer Records**

**Consents/Authorizations/Releases**
Resident Self Determination Act Acknowledgement
Living will
Durable Powers of Attorney
Guardianship/Conservator
Legal incapacitation
Consents/Acknowledgements/Releases

**Physician Progress Notes**

**Nursing Notes/Interdisciplinary Notes**

**Clinical Assessments**

**Medication, Treatment and Other Flowsheets**

**Lab, X Rays, and Special Reports**

**Rehabilitative Therapy (PT, OT, SLP)**

**Consultants**
Other specialists/consultations

**HIPAA Documents**
HIPAA Request and Response Log
Requests for Accounting of Disclosures
Requests for Amendment
Requests for Alternative Communication
Requests for Restriction of Access to PHI

**Miscellaneous**
Other Hospital Records (All hospital records received should be retained)
NOTE: RECORDS FROM OTHER HOSPITALS ARE FILED IN THE BACK OF THE RECORD

## SUBJECT: CENTRALIZATION OF PATIENT/RESIDENT INFORMATION

**POLICY:**
Medical Records maintains all current clinical information in each patient's/resident's clinical record.

**PROCEDURES:**

1. File all current information about the patient/resident in the patient's/resident's current active record.

2. Thin current overflow records as needed. Maintain this information in an accessible manner and available upon request.

## SUBJECT: LOST MEDICAL RECORD

## POLICY:

Should a record be misplaced, every effort will be made to locate the record or to reconstruct as much of the record as possible from copies of the records of individuals who charted in the record and who maintained copies of their reports.

## PROCEDURES:

1. Assign one person to locate a missing record.

2. Check the Maser Patient Index to determine the correct spelling of the patient's/resident's name, service dates and patient's/resident's number.

3. Start the search with the Medical Record Sign-out Log.

4. If the chart was removed from Medical Records, the chart should be logged on Medical Record Sign-out Log.

5. If there is a return date entry listed in the Medical Record Sign-out Log, search Medical Records.

6. If there is no return date entry listed in the Medical Record Sign-out Log, call the individual who last used the record.

7. If there is no entry in the Medical Record Sign-out Log relating to the missing record, notify the nursing units and departments to determine if someone took the record and failed to follow procedure.

8. Notify Administration that the record is missing.

9. Notify the Fundamental Administrative Services, LLC Legal Department as this may constitute a possible breach of protected health information.

10. Begin to reconstruct the clinical record:
    A. Document that the medical record is missing and the date - indicate that a duplicate record has been started.
    B. Prepare a new medical record folder and write "duplicate" on the folder, "original missing" and the date.
    C. Reprint documents from any computer systems.
    D. Contact physicians' offices request copies of any clinical record information. When information is received, record "duplicate-original missing" and the date on the document.

12. Continue to search. In most cases, the medical record re-appears in the normal course of business. When the original is found, destroy the duplicate.

13. Evaluate the system failure that resulted in the loss of records and implement corrective measures to prevent it from occurring again.

## SUBJECT: DISCHARGE CHART ASSEMBLY INSTRUCTIONS

## POLICY:

All discharged charts assembled in a standardized manner to provide that all documentation is accurate and appropriate.

## PROCEDURES:

1. The discharged medical records and accompanying documentation are collected. Medical Records assembles and analyses the discharged medical records within 5 days allowing time for completion of deficiencies within 30 days of discharge or the state defined timeframe for record completion.

2. Check the loose material for late reports.

3. The discharge chart is assembled in reverse chronological order according to order indicated in the *Chart Order Thinning* policy.

4. Each page is checked to determine that the patient's/resident's name is on the page. If the name is the same but patient/resident number is different, remove the page and retrieve the record that corresponds to the number.

5. If a wrong name is written on the page, read documentation prior to the page in question. Read the documentation after the page in question. If the notes on the page in question have entries by the same staff and the entries correspond to the entries prior to and subsequent to the misidentified page, Correct the page ID. If the page appears not to belong in the chart on which you are working, retrieve the chart of the patient/resident whose reports were not charted correctly and review that chart to determine if the report should be charted.

6. If the page is unidentified, verify with the specific discipline where page is kept in chart, if the page is for that particular patient/resident. After identifying notes follow the procedures outlined above.

7. The discharged chart is fastened together to prevent loss of documentation. Acceptable methods of fastening are:
   A. File folder with two-pronged metal fastener.
   B. Specialty fastener rubber bands designed to have a life-span equal to the retention period. Records should be fastened around both the length and wide of the pages.
   C. Pocket accordion folders in combination with a metal fastener or specialty rubber band.

8. The discharged chart is label with patient/resident full name, admission date, discharged date, medical record number and volume number (i.e. 1 of 3, 2 of 3, 3 of 3).

9. If the patient/resident has records from a previous stay, those records are pulled forward and placed behind the current discharged chart. Records from a previous stay are **not** integrated into the current discharged chart and are not re-fastened unless needed.

**SUBJECT: DISCHARGE CHART ASSEMBLY INSTRUCTIONS (Continued)**

10. Discharge chart folders are labeled consistently. Common label format includes:
    A. Patient/Resident full name
    B. Admit date (original AND readmit as applicable)
    C. Discharge date and disposition (home, hospital, other SNF)
    D. Volume #'s (volume 1 of 2, 2 of 2 etc…)

## SUBJECT: MEDICAL RECORD NUMBER ASSIGNMENT

### POLICY:

All patients/residents admitted will be assigned a unique facility number (patient/ resident Medical Record Number).

### PROCEDURES:

1. Upon admission, assign each patient/resident a unique patient/resident medical record number.

2. The medical record number may be automatically assigned by a clinical application in admission sequence.

3. Audit charts routinely for consistent use of patient/resident medical record numbers.

4. Keep documentation of all patient/resident medical record numbers in Medical Records.

**SUBJECT**: **DOCUMENTATION GUIDELINES**

**POLICY:**
Documentation guidelines pertinent to good clinical record practice will be followed by all individuals who document in the patient's/resident's record. A complete health picture of the patient/resident must be available to all disciplines contributing to patient/resident care.

**GUIDELINES:**

1. Print or write neatly and legibly.

2. Use proper spelling and grammar.

3. Use approved abbreviations and symbols – no ditto marks are permitted.

4. Use only blue or black ink.

5. Make all entries in chronological order and do not leave blank spaces between entries.

6. Date and sign all entries, including the first initial, last name and title of the writer.

7. All entries should be based on the writer's first-hand knowledge.

8. Do not include assumptions or hearsay except to document your discussion with a resident or other individual.

9. Entries are factual and objective. The present tense is normally used.

10. Do not chart on someone's behalf or add/correct/alter another person's entry.

11. Do not document an action before it took place.

12. Do not document an action that did not take place.

13. Do not use profane language.

14. Do not use disparaging remarks or criticisms about patients/residents, visitors, co-workers or other health care professionals.

15. Approved and standard method for correcting mistaken entries and incorporating late entries will be followed. (REFER TO: *Correction of Charting Errors*,)

## SUBJECT: DOCUMENTATION: CORRECTING OF CHARTING ERRORS

### POLICY:

All mistaken entries will be corrected in a standardized manner. Corrections and/or late entries should be made immediately and only when:

1 Important information must be added after completion of the original note;
2 Original notes were not written; or,
3 Something was misstated in the original entry.

### PROCEDURES:

1. When corrections are needed: do not erase or obliterate anything;
   A. Do not use white-out or any other type of correction fluid or tape;
   B. Write "void" above or beside the original words and include the current date and your initials;
   C. Legibly and neatly, make your correction.

2. When a late entry is needed:
   A. Add entry on first available line
   B. Clearly label it as a "late entry"
   C. Begin with recording the current date and time then clearly identify the date and time when the entry should have been done within the body of the late entry.

3. If, during the course of charting, review or processing, Facility personnel discovers inconsistencies and/or alterations in a patient's/resident's record, Administration is notified and, if warranted, an incident report is completed.