

SUBJECT: USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION - GENERAL RULES	REFERENCE #1001
	PAGE: 1 OF: 3
DEPARTMENT: ORGANIZATIONWIDE	EFFECTIVE:
APPROVED BY:	REVISED:

**POLICY:**

\_\_\_\_\_ shall protect the privacy of individual protected health information. Because of this, the amount of information accessible in response to a request for information is limited to the purpose or need for the information.

**PROCEDURE:**

- Determine if the request for individual protected health information is permitted. Permitted reasons include:
  - In response to a request for information by the patient
  - To carry out treatment, payment or healthcare operations after receiving a consent from the patient
  - To carry out treatment, payment or healthcare operations without a consent, if a consent is not required, as seen in:
    - An indirect treatment relationship with the individual
    - The individual is an inmate of correctional facility
    - An emergency situation and attempts to obtain consent occur as soon as reasonably possible
    - The healthcare organization is required by law to treat the individual, however, cannot gain consent until a later time
    - Attempts to obtain consent from an individual are unsuccessful because of communication barriers with the individual, and it is determined that the individual's consent to treatment is inferred from the situation
  - To provide care, treatment and services, to support training programs, to provide legal defense, or is the author of psychotherapy notes
  - To maintain a directory of individuals in its facility
    - The information in this directory is limited to:
      - ◆ The individual's name
      - ◆ The individual's location in the facility

SUBJECT: USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION FOR MARKETING	REFERENCE #1028
	PAGE: 1 OF: 1
DEPARTMENT: ORGANIZATIONWIDE	EFFECTIVE:
APPROVED BY:	REVISED:

**POLICY:**

- \_\_\_\_\_ shall not use or disclose protected health information for marketing without a disclosure, except:
  - If the marketing communication occurs in a face-to-face encounter with the patient
  - If the marketing communication concerns products or services of a nominal value
  - If the marketing communication concerns health-related products or services of the organization or of a third party
- The organization may disclose protected health information for the purposes of marketing communications to a business associate only if the business associate is assisting the organization with the marketing communication.

**PROCEDURE:**

- Marketing communications must:
  - Identify the organization as the source of the communication
  - State if the organization is going to receive, either directly or indirectly, any remuneration for the communication
  - Identify how a patient may opt-out of receiving any future types of communications
    - If the communication is contained within a newsletter or similar type of general communication that is distributed to a broad base of patients, employees or other individuals opting-out does not need to be provided.
- If the organization is using protected health information to target information specifically to a type of patient based upon their health status or condition:
  - The organization must determine that the communication about the product or service being marketed is beneficial to the health of the targeted patient population.
  - The communication has to explain why the patient has been targeted and how the product or service explained within the communication relates to the health of the patient.
- The organization ensures that patients who decide to opt-out of receiving any future marketing communications will not receive the communications effective of the opt-out date.

SUBJECT: ACCESS OF INDIVIDUALS TO PROTECTED HEALTH INFORMATION	REFERENCE #1038
DEPARTMENT: ORGANIZATIONWIDE	PAGE: 1 OF: 3
APPROVED BY:	EFFECTIVE: REVISED:

**POLICY:**

- \_\_\_\_\_ shall supply protected health information to patients upon request.
  - Information that is not supplied to the patient includes psychotherapy notes or any information compiled for use in a court of law.
  - The organization may deny providing a patient a copy of his/her protected health information if the patient is an inmate of a correctional facility and if the information could jeopardize the health, safety, security, custody or rehabilitation of the patient or other inmates, or the safety of any officer, employee or other person at the facility responsible for the transportation of the inmate.
  - A patient may be denied access to his/her protected health information if the patient is involved in research that includes treatment and he/she has consented to not have access to his/her protected health information while the research is in progress. Access to the protected health information will resume upon completion of the research.
  - A patient may be denied access to his/her protected health information if the information was obtained from a source other than the organization with the promise of confidentiality.

**PROCEDURE:**

- If a patient requests to read or wants a copy of his/her protected health information:
  - Determine if the patient has any grounds for the request to be denied.
    - An employee determines that the patient’s life or physical safety might be in jeopardy if he/she have access to his/her protected health information.
    - Another person’s life or physical safety might be in jeopardy if the patient has access to his/her protected health information.
    - The information contains reference to another person and this information could cause harm to that person.
    - The request is made by the patient’s personal representative and the employee has determined that permission could result in harm to the patient or another person.

SUBJECT: ADMINISTRATIVE SAFEGUARDS - WORKFORCE AUTHORIZATION/ SUPERVISION	REFERENCE #2012
	PAGE: 1
DEPARTMENT: ORGANIZATIONWIDE	OF: 1
	EFFECTIVE:
APPROVED BY:	REVISED:

**POLICY:**

- \_\_\_\_\_ shall authorize and supervise staff who work with electronic protected health information.
- Individuals/departments are identified with specific policies/procedures defining the degree of access and need for protected health information.

**PROCEDURE:**

- Information Systems Department/Systems Administrator staff shall have access to all documentation present in the medical record.
- Nursing Services Department staff shall have access to all pertinent patient information to allow for optimum assessment, treatment and care of the patient in accordance with general nursing policies and procedures.
- Medical staff shall have access to all pertinent patient information that will allow them to provide optimum treatment to any patient for which they are attending, covering or serving as a consulting physician in accordance with the medical staff performance expectations.
- Clerical personnel categorized as Business Office staff shall have access to all necessary patient information that allows for appropriate billing, insurance and financial procedures.
- Performance Improvement, Utilization Management, Case Management and/or Risk Management Department personnel shall have access to all pertinent patient information, both clinical and financial, to allow for optimum assessment to perform the expected function within the department.
- All other ancillary and administrative personnel shall have access to patient information on an as needed basis, restricted to level of authority, according to organizationwide policies and procedures which govern the security and confidentiality of patient information.

SUBJECT: PHYSICAL SAFEGUARDS - DEVICE AND MEDIA CONTROLS - DATA BACKUP AND STORAGE	REFERENCE #2047
	PAGE: 1
DEPARTMENT: ORGANIZATIONWIDE	OF: 2
	EFFECTIVE:
APPROVED BY:	REVISED:

**POLICY:**

\_\_\_\_\_ shall backup and store electronic protected health information while being used within the organization, so that an exact copy of electronic protected health information can be created, if necessary.

**PROCEDURE:**

- The organization’s leadership will determine the conditions in which a replication of electronic protected health information may need to be created. This list will be given to the Information Systems Department Director/Systems Administrator.
- The list of conditions will be reviewed prior to removing or storing any equipment.
- Specific employees identified by the Information Systems Department Director/Systems Administrator are responsible for backing up and storing electronic protected health information. These employees are:

_____	_____
_____	_____
_____	_____
_____	_____

- These employees are responsible for:
  - Logging when protected health information was backed up and stored
  - Recreating electronic protected health information before moving, removing or relocating a piece of hardware, if required
  - Creating electronic tape backups of the computer systems
  - Labeling the data backup tapes; ensuring safe delivery of the tapes to the off-site storage facility