HIPAA PRIVACY

New Policy: 11/2014
Committee Review: 01/2015

POLICY

It is the policy of the Company to comply with the Company responsibility to protect individually identifiable health information and the system components that is defined in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the security and privacy regulations implementing HIPAA, other federal and state laws protecting confidentiality of health information, professional ethics, and accreditation requirements.

This Permitted Uses and Disclosures policy governs uses and disclosures of Protected Health Information (PHI) that are permitted under HIPAA with or without the need for an individual's consent, authorization or verbal agreement. Demonstrated competence in the requirements of this policy is an important part of every employee's responsibilities.

The complete Permitted Uses and Disclosures policy is available at the Corporate Office.

DEFINITIONS

Protected **Health Information (PHI)** is individually identifiable health information, whether oral or recorded in any form or medium, that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse which relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
    a) That identifies the individual; or
    b) With respect to which there is a reasonable basis to believe the information can be used to identify the individual."

Covered Entity is a health care provider or a health care clearinghouse (public or private) which either processes or facilitates the processing of health information.

Business Associate is an individual or corporate "person" that performs on behalf of the covered entity any function or activity involving the use or disclosure of PHI and is not a member of the covered entity's workforce.

Responsible Party is the individual(s) who has been deemed by the appropriate authorities to consent to the disclosure of PHI in the event that reasonable professional judgment has determined that the patient is unable to provide said consent.

Company workforce

For purposes of this Policy, the company's workforce includes individuals who would be considered part of the workforce under HIPAA such as employees, volunteers, trainees, and other persons whose work performance is under the direct control of the company, whether or not they are paid by the company.

PROCEDURES

All responses to requests for PHI will be limited to the minimum amount of information needed to accomplish the purpose of the request or disclosure. An individual may authorize use, request restrictions, inspect his or her records by making a request according to the appropriate protocols, and amend and request an accounting of disclosures of his or her PHI. The Permitted Uses and Disclosures policy describes in more detail how an individual's PHI may be used and disclosed.
The Compliance Committee will assist in the interpretation of all laws and regulations related to this Policy, the procedures and practices, and will guide the contact person and company in their implementation.

ONR and its employees shall use or disclose protected health information as follows:

- To the individual or responsible party.
- Pursuant to carry out treatment, payment, or health care operations.
- As a result of a request by a health care provider for treatment.
- The information is requested by another covered entity or business associate.

MAINTAINING SECURITY

- Employees are to be given access only to the information required to perform their job.
- Do not leave PHI information, records, or materials in a public area.
- Do not share passwords and/or allow anyone access to your computer.
- Always lock your computer when not in use.
- Do not log on to a PHI program and then leave your computer unattended.
- Do not modify or copy PHI without authorization.
- Do not discuss PHI in a place where the conversation can be heard by unauthorized persons.
- Do not discuss PHI with an unauthorized person.
- Disclosing or using PHI in an unauthorized manner.
- Cooperate with the HIPAA privacy officer.
- Do not obtaining PHI under false pretenses for personal gain.
- Electronic Communication (communication transmitted by electronic media; maintained in electronic media; [texting] or transmitted or maintained in any other form or medium.)
    - "Omitting a patient's name does not guarantee that the person cannot be identified. The uniqueness of a medical condition combined with the time and date of a visit could be enough for people to identify a patient."
    - Resident's initials may be used only when absolutely necessary.
    - Limit the information as much as possible. Keep it simple and generic (what HIPAA likes to call "de-identified information")—*for example, "Room 428 is ready for discharge."*
    - Do not add commentary.
    - If necessary, for clarification and avoidance of error, the text may identify a room number or area where information is available - *for example, "See JH, room 210".*
    - Use caution when replying to an electronic communication.
        - It is your responsibility to confirm and/or delete any previous communication included in the email when responding or forwarding the information.
        - When "reply all" is used, only include persons you know are authorized to receive the communication.
    - When including attachments in an electronic communication, send only as a secure attachment.
- Patient photos may not be posted on public media for any reason without a written authorization from a resident or their responsible party and written consent or agreement from the facility.

REVIEW

The Compliance Committee will review on an on-going basis the viability of the security policies and general approaches taken in the security procedures. The Compliance Committee will develop and recommend any necessary security policy or procedure changes.

The technical and non-technical viability of the security policies will be evaluated by the Compliance Committee

Any member of the HIPAA security committee, the HIPAA security office, or any other person may suggest changes to the security policies or procedures by submitting such suggestion to the HIPAA security committee for consideration.

In the event that one or more of the following events occur, the policy evaluation process will be immediately triggered:

- Changes in the HIPAA security or privacy regulations.
- New federal, state, or local laws or regulations affecting the privacy or security of PHI.
- Changes in technology, environmental processes, or business processes that may affect HIPAA security policies or security procedures.
- A serious security violation, breach, or other security incident occurs.

The company has a progressive discipline policy under which sanctions become more severe for repeated violations. These infractions constitute grounds for disciplinary action up to and including termination and criminal prosecution. However, the company reserves the right to terminate on the first breach of the HIPAA privacy rules.