LHC GROUP, INC.	PRIVACY AND SECURITY SANCTIONS
EFFECTIVE DATE: 04/20/2005	DIVISION: LHC ADMINISTRATIVE
REVISED DATE: 11/01/2014	CHAPTER: HIPAA PRIVACY RULE
APPROVED BY: POLICY COMMITTEE	POLICY NUMBER: 13.1.017
	PAGE 1 OF 4

PURPOSE:

To establish and document compliance with:

- HIPAA Privacy and Security Rule requirements in regards to required workforce member sanctions, retaliation prohibitions, and whistleblower protection standards; and,
- Applicable Sarbanes-Oxley Information Technology control standards.

POLICY:

LHC Group and its entities will:

- Provide required training to ensure all members of our workforce are knowledgeable about our privacy and security policies and procedures;
- Consistently apply appropriate sanctions uniformly across all workforce members who commit violations;
- Apply sanctions which include verbal warning, written warning, suspension, or termination of employment or business relationship;
- Shall assure no member of our workforce is permitted to intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for:
  - The exercise by that individual's right under federal and state privacy regulations;
  - Filing complaints (including providing minimally necessary protected LHC Group information);
  - Testifying, assisting, participating in an investigation, compliance review, proceeding, or hearing; or
  - Otherwise reasonably opposing in good faith any act or practice made unlawful by HIPAA privacy and security regulations.

DEFINITIONS:

Workforce Member: For the purposes of this policy, "workforce member" means employees, contract workers, volunteers, trainees, and other persons whose conduct, in the performance of work for the facility, is under the direct control of the facility, whether or not they are paid by the facility.

Negligent Violations - accidental/inadvertent and/or due to lack of proper education or an unacceptable number of previous violations

Intentional Violations – purposeful or deliberate violation of privacy or information security policies or an unacceptable number of previous violations.

PROCEDURE:

This section describes methods for determining the response to a privacy and/or information security violation. The procedure includes examples of violations, information to be considered and a range of appropriate sanctions. Sanctions will vary based on the nature and severity of the violation and the type of violation. The Human Resource Department should be consulted as needed, and will always be involved in possible workforce member terminations.

When a workforce member is reported for committing a privacy or security violation, an immediate investigation will be conducted by the Director of Privacy, in conjunction with the appropriate members of management or other designees, to determine the nature and severity of the violation.

During the entire investigation for each case, all managers involved shall assure strict adherence to our policies regarding retaliation prohibitions and whistleblower protections.

Appropriate sanctions will be determined based on the nature of the violation, its severity and whether it was negligent (accidental/inadvertent) or intentional. For systems security violations, The Director of Privacy and / or the Information Security Manager may temporarily or permanently change or revoke system privileges based on the violation severity and intention, with or without warning.

When determining the nature of the violation, questions to consider are:

- What is the severity of the privacy/security incident?
    - What type of information was inappropriately accessed, used, or disclosed (*e.g.*, was the protected health information (PHI) considered sensitive)?
    - How many patients were affected?
    - To what degree was a patient harmed?
    - To what degree was the confidentiality, integrity, and/or availability of systems or data impacted?
    - To what degree did the action place the computer systems or network at risk?
- Was the inappropriate action negligent (accidental/inadvertent) or intentional?
- Did the inappropriate action cause harm or is it likely to cause harm to a patient or others?
- To what degree were details of the situation verified through audit trails, interviews, or other facts?

In addition to the nature of the violation itself, answers to the following questions may affect the severity of disciplinary action:

- How long has the workforce member been employed?
- What is the workforce members' past work record?

- What is the workforce member's quality of service to the facility?
- Has the workforce member been disciplined for prior HIPAA privacy or security violations in the past?
- Does the workforce member have any written warnings for HIPAA privacy or security violations in his or her HR file?

Any actions that indicate a workforce member's lack of focus on and commitment to basic privacy and security principles could result in termination, regardless of all other aspects of the workforce member's past performance and/or work history. In addition, referrals to law enforcement may be made for incidents of stealing information from company systems to commit identity theft, and to investigate incidents involving accessing inappropriate material on the Company network, depending on the nature of the material accessed.

The sanctions taken against workforce members may vary with the specific circumstances related to the violation. For negligent (accidental or inadvertent) violations, sanctions may include re-training and counseling, a written warning, an action plan, suspension or termination from the workforce, depending on the circumstances. For intentional violations, sanctions may include a written warning, an action plan, suspension or termination from the workforce, depending on the circumstances.

Any sanctions applied will be documented and retained in the workforce member's file for a period of ten (10) years.

Examples of privacy and security violations:

- Inappropriate access, use, disclosure, or disposal of sensitive information
- Sending sensitive information via mail, email or fax to a non-authorized individual or the wrong provider
- Improper protection of sensitive information
- Failure to properly sign-off a workstation
- Failure to properly safeguard username and passwords and/or sharing passwords
- Opening an attachment in an unexpected email from an unknown third party resulting in the computer becoming infected with a virus
- Accessing one's own PHI in any system
- Leaving detailed sensitive information on an answering machine
- Not properly verifying individuals by phone, in person or in writing
- Failure to properly handle a request for confidential communications
- Misusing the Company network to view inappropriate material
- Intentionally bypassing Company network security controls for unauthorized reasons
- Posting sensitive information on the internet

- Photographing a patient within the facility for personal use
- Sale of sensitive information to any source
- Stealing sensitive information to commit identity theft
- Texting patient health information.
- Disabling information security tools, bypassing security measures, and misusing tools that can compromise information security systems (*e.g.*, deliberately compromising electronic information security measures)