PRIVACY 29.0 FACILITY SANCTIONS POLICY

Scope: All workforce members, including employed medical staff, employed by any subsidiaries of Universal Health Services, Inc., including facilities and UHS of Delaware Inc. (collectively, "UHS").

Purpose: To establish a sanction policy under which Facilities will apply appropriate counseling and sanctions against members of their workforce who fail to comply with the Facility's policies and procedures, federal, state, or local law, regulatory requirements, etc.

Policy:

Facilities are required to have and apply appropriate sanctions against members of their workforce who fail to comply with Facility policies and procedures, violate local, state, or federal law, or whose actions cause infractions against their professional license. Sanctions may include but are not limited to infractions against professional licensure, certification, registration, criminal history convictions, history of child abuse, managed care organizations, Medicare, Medicaid, or any other Company payor or provider, and violations of HIPAA Privacy Rule. Violations will lead to corrective action, the severity of which will depend on the circumstances of the violation.

Corrective actions may take place in several forms. The forms of actions are preventive counseling, written warning, final written warning, and/or immediate employment termination. The Facility's CEO/Managing Director or designee and Human Resource Department should be consulted beforehand when action is necessary.

Procedure:

Below are guidelines to be used by Facilities in developing and applying appropriate counseling and sanctions. The actions should be consistent with applicable UHS Human Resources and Facility policies and procedures, which may or may not incorporate procedures from the medical staff bylaws, including any applicable employment agreement.

Guidelines

The Facility expects all employees to comply with the organization's standards of behavior and performance and to know that any noncompliance with these standards must be remedied. The Facility prefers to attempt to correct unacceptable behavior or unsatisfactory performance through a corrective action process. However, the Facility reserves the right to by-pass any corrective action step(s) and impose the degree of discipline, including immediate employment termination, which it deems appropriate in the sole discretion of the Facility. It is also understood that there are certain rules of conduct that are so important that their violation usually should lead to the offender's immediate employment termination.

The usual process for the corrective action process is:

- Preventive Counseling
- Written Warning
- Final Written Warning
- Employment Termination

The Facility policy for corrective action must be consistent with UHS Corporate Policy H.R. 27.0 *Corrective Action Process*.

Violations of the HIPAA Privacy Rule

Facilities are required to have and apply appropriate sanctions against members of their workforce who fail to comply with Facility privacy policies and procedures or the requirements of the HIPAA Privacy Rule. Violations may lead to disciplinary action up to and including immediate employment termination, the severity of which depends on the circumstances of the violation. Facilities should use the guidelines listed below in developing and applying their sanctions policy.

Violations of Facility privacy policies and procedures or the HIPAA Privacy Rule may be categorized as follows:

Level 1 -- Careless or Inadvertent Violations

Level 1 violations occur when workforce members unintentionally or carelessly access, review, or reveal PHI to himself/herself or others without a legitimate "need to know."

Examples include, but are not limited to:

- Workforce member discusses PHI in a public area;
- Workforce member leaves a medical record unattended in an accessible area within the Facility;
- Workforce member fails to log off a computer terminal or shares a password.

Depending on the circumstances, even when the basis for the violation is careless (such as an accidental loss of PHI), the violation may be considered more serious and elevated by one or more levels. (For example, misplacing electronic or paper records containing PHI of multiple individuals off the premises of the Facility that are never recovered may lead to more serious disciplinary action than misplacing a single patient's records from a Facility-based location and recovering the records within a shorter period of time.)

Level 2 -- Curiosity or Concern (no personal gain)

This level of violation occurs when a workforce member intentionally accesses or discusses PHI for unauthorized purposes, for reasons unrelated to personal gain.

Examples include but are not limited to:

- Workforce member looks up birth dates or addresses of friends or relatives;
- Workforce member accesses and reviews a record of a patient out of concern or curiosity;
- Workforce member reviews a public personality's record.

Level 3 -- Personal Gain or Malice

This level of violation occurs when a workforce member accesses, reviews, or discusses confidential patient information for personal gain or with malicious intent.

Examples include but are not limited to:

- Workforce member reviews a patient record to use information in a personal relationship;
- Workforce member gathers patient information to be sold.

Investigation

Upon receipt of a report of a violation or suspected violation, the following investigation(s) shall occur:

- For employed individuals, the Privacy Officer conducts an investigation in cooperation with the Facility's Human Resources department, the employee's supervisor or designee. For employed physicians, the Medical Staff Office (or other applicable office) will also be apprised of the investigation. In most cases, a final report is to be prepared by the Privacy Officer and submitted to the employee's supervisor and the Facility's Human Resources department, with the results of the investigation and any recommendations for corrective action and/or sanctions.

- For non-employee physicians and other allied health professionals subject to a contract and/or the medical staff bylaws, the Privacy Officer conducts an investigation in cooperation with the Human Resources department and Medical Staff Office (or other applicable office), and provide them with a final report with the results of the investigation and any recommendations for corrective action and/or sanctions.

- For volunteers, the Privacy Officer conducts an investigation. A final report is prepared by the Privacy Officer to the Facility's Human Resources department and volunteer office (if any), setting forth the results of the investigation and any recommendations for corrective action and/or sanctions.

- For other workforce members, including business associates, contracted employees and other workforce members, the Privacy Officer obtains a copy of the business associate agreement or other applicable contract and conduct an investigation. A final report is prepared by the Privacy Officer to the Facility's primary contact and their department head.

Sanctions

Sanctions involving employees shall be addressed in accordance with applicable Human Resources policies and procedures. All other disciplinary actions are handled in accordance with applicable Facility or Human Resources policies and practices, medical staff bylaws and contract terms. The UHS Legal department may be consulted in determining the appropriate disciplinary action to be taken when an employment agreement, business associate agreement or other contract applies to the relationship.

Documentation

The Privacy Officer or his/her designee will document the investigations and sanctions that are applied. A copy of the documentation will be retained by the Privacy Officer or designee for six (6) years.

Related UHS Policies:

UHS H.R. 27.0 *Corrective Action Process*

Revision Dates:	**10-12-2017; 11-16-2015; 07-22-2013**
Implementation Date:	**08-19-2011**
Reviewed and Approved by:	
UHS Compliance Committee	