PURPOSE:
The purpose of this Compliance Misconduct and Sanction Policy (the “Policy”) is to establish that disciplinary Sanctions will be applied against Health Quest Systems, Inc. and its affiliates’ (“HQ”) Workforce Members who fail to comply with federal and state laws and regulations, the Code of Conduct policies and procedures for compliance, privacy and security of protected health information (“PHI”) or who engage in behavior that may result in a compliance or privacy violation. This policy applies to all Workforce Members, which include employees, independent contractors, agents, volunteers, trainees, or other persons who perform work for or on behalf of HQ.

POLICY:
It is the policy of HQ to fairly and consistently apply Sanctions to Workforce Members who fail to abide by federal and state laws and regulations; the Code of Conduct; compliance, privacy and security policies and procedures; or who engage in behavior that may result in a compliance or privacy violation. Sanctions will be administered to Workforce Members for (1) failing to report suspected problems; (2) participating in noncompliant behavior; or (3) encouraging, directing, facilitating or permitting noncompliant behavior. Misconduct will result in appropriate and immediate remediation and/or disciplinary action, up to and including termination of any employment or other work arrangement or business relationship with a Workforce Member. Disciplinary action will be based upon the type and severity of the misconduct, the relationship with the Workforce Member, the disciplinary record of the individual involved, and any existing collective bargaining agreements.

DEFINITIONS:
Director/Manager: An HQ employee responsible for directing or managing day-to-day operations.

Sanctions: Disciplinary action issued for determined compliance misconduct.

Workforce Members: Any employee, independent contractor, agent, volunteer, trainee, or other person who performs work for or on behalf of HQ. This includes: full-time, part-time, and pool employees; associates; directors; officers; managers; supervisors; volunteers; members of the Board and members of standing committees; medical staff employed by or otherwise affiliated
with HQ; affiliated students or others receiving training at any HQ facility; and others who provide goods or services to HQ.

POLICY STATEMENT:

1. The failure to comply with federal and state laws and regulations, the Code of Conduct, policies relating to compliance, privacy or security of PHI and other sensitive information ("misconduct") or behavior that may result in a compliance or privacy violation by a Workforce Member will result in Sanctions consistent with this Policy, Human Resources’ Disciplinary Policy and Medical Staff Bylaws.

2. Directors/Managers who fail to detect or report misconduct on the part of a Workforce Member under their supervision shall be subject to Sanctions. Failure to detect misconduct means that the supervisor knew about the misconduct but failed to identify the misconduct as potential misconduct involving federal and state laws and regulations, or the Code of Conduct, or compliance, privacy and security policies and procedures.

3. Compliance misconduct involving medical staff members will be referred to the appropriate HQ Chief Medical Officer or VP of Medical Affairs for Sanctions consistent with Medical Staff Bylaws.

4. Compliance misconduct involving any other Workforce Members will be referred to the appropriate HQ Manager for Sanctions consistent with this Policy.

5. HQ may terminate the employment, contractual or other relationship with an HQ Workforce Member without first resorting to less severe forms of discipline for misconduct involving federal and state laws and regulations, the Code of Conduct, policies and procedures for compliance, privacy and security of PHI or behavior that may result in a compliance or privacy violation.

6. For misconduct involving federal and state laws and regulations, the Code of Conduct, policies and procedures for compliance, privacy and security of PHI, or behavior that may result in a compliance or privacy violation, appropriate Sanctions will be in consultation with Compliance, Human Resources, the General Counsel, and/or management, as appropriate. Management or Human Resources, as appropriate, is responsible for executing the Sanctions and/or corrective measures, and issuing a written report to the Chief Compliance Officer documenting the Sanctions and/or corrective actions. The Chief Compliance Officer, the General Counsel, or their designees may be involved in investigating misconduct and in following up to determine that proper Sanctions and/or corrective action have been taken. For all other misconduct under this Policy, management and/or Human Resources, as appropriate, is responsible for
applying disciplinary Sanctions in accordance with this Policy, the Human Resources’ Disciplinary Policy and Medical Staff Bylaws, and issuing a written report to the Office of Compliance, Internal Audit and Privacy (“OCIAP”) documenting the Sanctions imposed and completion of corrective action. The Chief Compliance Officer, or a designee, may follow up to determine that proper Sanctions and/or corrective actions have been taken.

7. Compliance misconduct may also result in notification to law enforcement officials and/or regulatory, accreditation and licensure organizations.

CATEGORIES OF COMPLIANCE MISCONDUCT AND SANCTIONS:

Categories of Compliance Misconduct:
The following guidelines have been established to provide consistency when determining Sanctions for compliance misconduct. The level of Sanction will depend on the severity of the misconduct, whether there have been previous transgressions, and a review of the employee’s personnel file. The misconduct listed below, while not all inclusive, are organized according to the severity. Decisions may be made on a case-by-case basis, and any deviations from the guidelines should include consultation with the Chief Compliance Officer or designee.

Categories of Compliance Sanctions:
The failure to comply with federal and state laws and regulations, the Code of Conduct, policies and procedures for compliance, privacy and security of PHI, or behavior that may result in a compliance or privacy violation will include Sanctions up to and including termination of employment. Other Sanctions may include, but are not limited to, termination of a contract, suspension of the right to access PHI and other sensitive information, and termination of other privileges.

Category 1 Description: Improper and/or unintentional disclosure of confidential information. This level of misconduct occurs when PHI, sensitive information or confidential HQ information is unintentionally or carelessly disclosed to others who do not have a “need to know” within the normal course of legitimate business or patient care activities.

Category 1 Sanctions: (First Offense)
Sanctions will follow this Policy and Human Resources’ Disciplinary Policy around disciplinary action and will include appropriate Compliance/Privacy/PHI Security training and may include:
  i. Written Caution or documented counseling to associate’s personnel file.
  ii. Repeated offenses may result in progressive discipline.

**Category 2 Description:** Intentional acts of noncompliance. Category 2 misconduct may also include any repetition of Category 1 or 2 misconduct.

This category of compliance misconduct may include, but is not limited to: providing free or discounted services to patients without prior authorization; manager’s receiving a report of noncompliance from staff and failing to report such an event to OCIAP; unauthorized use, misuse or access of PHI or records (e.g., inappropriate access of the PHI of a family member or co-worker; looking up birth dates, addresses of friends or relatives; access of anyone’s record out of curiosity or concern; accessing the Workforce Member’s personal medical record on Health Quest’s electronic health record systems, failing to safeguard computing device or application passcode that may result in another individual violating a patient’s rights to privacy).

**Category 2 Sanctions: (First Offense or Repeated Category 1 Offenses)**
Sanctions will follow this Policy and Human Resources’ Disciplinary Policy around disciplinary action and will include appropriate Compliance/Privacy/PHI Security training and may include:
  i. Written Warning to personnel file.
  ii. Repeated offenses may result in progressive discipline.

**Category 3 Description:** This level of misconduct occurs when a Workforce Member acts in deliberate or reckless disregard of HQ policies and procedures or federal or state laws for personal gain or to expose HQ to fraud, waste or abuse claims.

This category of compliance misconduct may include but is not limited to: using PHI in a personal relationship where the disclosure is intended to damage or embarrass; sale of data for personal gain; billing for a service that was not rendered to increase revenue; solicitation of gifts from vendors or patients; or paying a referral source to provide referrals.

**Category 3 Sanctions: (First Offense or Repeated Category 2 Offenses)**
Sanctions will follow this Policy and Human Resources’ Disciplinary Policy around disciplinary action and will include suspension or termination of employment. Other penalties may include:

ii. Civil penalties as provided under HIPAA or applicable federal/state law

iii. Criminal penalties as provided under HIPAA or other applicable federal/state law

REFERENCES:
United States Sentencing Commission, Guidelines Manual, Ch. 8 (Nov. 2015).
HIPAA Administrative Control 45 CFR § 164.308 (a) (1) (ii) (C) and 164.530 (e) (1)
HITECH, Subpart D 164.414 (a)
NIST SP800-53 R2 PS-8
New York State Social Services Law § 363-d, 18 NYCRR §521
5.1.23 Compliance Misconduct and Sanctions Procedure

POLICY HISTORY:
Supersedes: 3/13/19
Original Implementation Date: 2/14/18
Date Reviewed: 3/9/20
Date Revised: 2/14/18, 3/13/19, 3/9/20

APPROVAL:

[Signature]
Policy Owner: W.A. McNulty
Date: 3.31.20