ADMINISTRATIVE POLICY

SUBJECT: Patient Safety Organization (PSO)

POLICY: All collection, management, analysis and communication of the patient safety information are to be handled according to this policy.

PURPOSE: Patient Safety information is considered confidential and must be handled as such. The XXX Team Members must follow this policy to ensure the appropriate collection and management of patient safety information is done according to laws, regulations and policy.

ADMINISTRATIVE RESPONSIBILITY: The Vice President – General Counsel is responsible for interpreting this policy. The Director of Quality is responsible for administering this policy. All Team Members are accountable for policy compliance.

DEFINITIONS:
Patient Safety Evaluation System (PSES): The means for the collections, management, analysis, and communication of information for reporting to or by a PSO. The PSES may include information about events, errors, near-misses, quality improvement data, and other patient safety data and information that is developed by and for the PSES workgroup, and is investigated, examined, and analyzed by the workgroup.

Patient Safety Work Product (PSWP): Documentation that reflects the deliberations and analysis surrounding patient safety and quality improvement activities that are performed within the PSES. PSWP may be data, reports, records, memoranda, analysis, or written or oral statements involved in the development of data and information for reporting to the PSO.

1. Identifiable Patient Safety Work Product: PSWP that includes identification of any provider that is a subject of the work, or any providers that participate in activities that are a subject of the work. It may also be considered identifiable because if contains patient-identification information which would invoke the HIPAA confidentiality regulations or that identifies the individual who reported information in good faith.
2. Non-identifiable Patient Safety Work Product: Anonymous as to provider, de-identified as to protected health information, and contextually de-identified so that the provider, patient or reporter cannot be identified.
3. The following cannot be PSWP:
    - The patient's medical record
    - Billing and discharge information
    - Other original patient or provider information
    - Data and reports generated for submission to external agencies to meet mandatory or voluntary reporting requirement.
    - Improvements, process and policy changes, and Action Plans made as a result of work within the PSES or the PSO.

4. Non-PSWP
    - Items that have not been reported to the PSO and are voluntarily removed from the organization's PSES by the Director of Quality.
    - Items clearly identified by policy or in writing on the documents as non-PSWP by the VP – General Counsel or the Director of Quality and submitted to the PSES for reporting to the PSO, or are reported through other channels to the PSO.
    - Information collected, maintained or developed separately from the PSES
    - Deliberations and analysis performed outside of the PSES unless it is subsequently submitted to the PSO.
5. Information that is non-PSWP, even if it resides in the PSES or has been reported to the PSO, is not protected.
6. Data and information that is designated as PSWP within the PSES cannot be voluntarily removed from the PSES and re-designated as non-PSWP once deliberations and analyses have begun about the information or events it reflects.
7. PSWP is accessible only to the member of the XXX workforce who needs it to perform their job functions.

Patient Safety Activities: Efforts to improve patient safety and the quality of healthcare delivery, including the collection and analysis of PSWP.

Workforce: Information about patient safety events is reported to the members of the workforce as necessary to meet the expectations for the risk management, quality and safety activities defined by XXX.

PSES Workgroup: XXX defines PSES workgroup as established Committees, Teams and Quality/Risk assigned groups who routinely perform patient safety and quality analysis and improvement work. Other individuals with special subject matter expertise may be called upon as deemed necessary by the Director - Quality for work on specific events or issues.

Submission of Information to the PSES: Information collected for submission to the PSES is considered to be PSWP at the time it is collected or developed, unless specifically designated as non-PSWP by the Director – Quality. The data/information is submitted to the PSES as part of the PSO reporting process.

- Non-PSWP submitted to the PSO must be identified as such and is not protected under the PSQIA.

Access to Information within the PSES:
Identifiable PSWP is accessible only to members of the organization's workforce as needed to perform their job function.

- Access to electronic PSWP that has been entered or uploaded into PSO data system will be made available through secure and unique user IDs and passwords.
- Access to other electronic files containing PSWP will be limited by using a designated username and password-protected data system or folder on the designated server.
- Paper PSWP documents will be stored in the offices of Risk Management in a locked storage file, and is only accessible by the VP – General Counsel, Director – Quality and the Risk Management Team.

- Requests for access to the PSWP and information held within the PSES are determined by the VP – General Counsel.

Confidentiality and Protection of PSWP:
XXX considers all data and information collected as PSWP to be confidential and protected under the PSQIA.

- All individuals defined as workforce members within the PSES will maintain the confidentiality of PSWP.
- The terms of the applicable confidentiality agreements signed by the workforce will survive after the completion or termination of their relationship with the organization.

Maintenance of PSWP within the PSES:
PSWP will be maintained in designated locations that allow for appropriate confidentiality and security, such as locked file cabinets; and/or secure electronic files and folders, or components of other software programs dealing with risk management, quality and safety, such as incident reporting systems, which are located separately from non-PSWP or otherwise designated as PSWP. PSWP may also be maintained within the data system provided to the organization by its contracted PSO and designated as a component of XXX's PSES.
Director - Quality is responsible for maintaining member access privileges to PSWP.

Submission of PSWP to the PSO:
XXX will review information contained within the PSES and determine what will be submitted to the PSO. Data and information submitted to the PSO, unless designated as non – PSWP before submission, must be treated as confidential PSWP.

Disclosures: Identifiable PSWP shall not be disclosed except as permitted by the PSQIA. Any disclosure will be managed by the Director - Quality.

Breach of Confidentiality:
In the event of an unauthorized disclosure or breach, XXX will follow the XXX policy HIPAA Privacy Breach Determination and Notification.

XXX Committee:
Reviewed:
Revised:
Replaces:
References: Patient Safety and Quality Improvement Act of 2005 (PSQIA): available at http://www.pso.ahrq.gov/statute/pl109-41.pdf) and the Final Regulation, 42 CFR Part 3 available at http://www.pso.ahrq.gov/rulemeking/nprmtx01.pdf.

HIPAA – Regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 as amended by the American Recovery Reinvestment Act of 2009, Title XII "Health Information Technology for Economic and Clinical Health Act"