ALLIED CARE EXPERTS
ACE
MEDICAL CENTER
ILOILO
A member of ACE Group of Hospitals
BRGY. UNGKA, JARO ILOILO CITY

ANNEX B

ENTERPRISE RISK MANAGEMENT FRAMEWORK

Enterprise Risk Management (ERM) is a process, affected by ACEMCI's Board of Directors, Management, and other personnel. This process is applied in strategy setting and across the Company, designed to identify potential events that may affect the company, and manage risks to be within its appetite.

ERM provides reasonable assurance regarding the realization of the Company's goals. ACEMCI can identify, assess, respond and monitor the outcomes of the industry's leading risk factors with an Enterprise Risk Management system in place.

Risk Management is a business routine in the hospital industry. The following are the identified risks:

OPERATIONAL RISKS

The business of healthcare is the delivery of care that is safe, timely, effective, efficient, and patient-centered within diverse populations. Operational risks relate to those risks resulting from inadequate or failed internal processes, people, or systems that affect business operations. Included are risks related to: adverse event management, credentialing and staffing, documentation, chain of command, and deviation from practice.

CLINICAL PATIENT SAFETY

Risks associated with the delivery of care to residents, patients and other healthcare customers. Clinical risks include: failure to follow evidence based practice, medication errors, hospital acquired conditions (HAC), serious safety events (SSE), and others.

STRATEGIC RISKS

Risks associated with the focus and direction of the organization. Because the rapid pace of change can create unpredictability, risks included within the strategic domain are associated with brand, reputation, competition, failure to adapt to changing times, health reform or customer priorities. Managed care relationships/partnerships, conflict of interest, marketing and sales, media relations, mergers, acquisitions, divestitures, joint ventures, affiliations and other business arrangements, contract administration, and advertising are other areas generally considered as potential strategic risks.

FINANCIAL RISK

Decisions that affect the financial sustainability of the organization, access to capital or external financial ratings through business relationships or the timing and recognition of revenue and expenses make up this domain. Risks might include: costs associated with malpractice, litigation, and insurance, capital structure, credit and interest rate fluctuations, foreign exchange, growth in programs and facilities, capital equipment, corporate compliance (fraud and abuse), accounts receivable, days of cash on hand, capitation contracts, billing and collection.

HUMAN CAPITAL

This domain refers to the organization's workforce. This is an important issue in today's tight labor and economic markets especially with the current brain-drain of health workers. Also included are risks associated with employee selection, retention, turnover, staffing, absenteeism, on-the-job work-related injuries (workers' compensation), work schedules and fatigue, productivity and compensation. Human capital associated risks may cover recruitment, retention, and termination of members of the medical and allied health staff.

LEGAL/REGULATORY

Risk within this domain incorporates the failure to identify, manage and monitor legal, regulatory, and statutory mandates. Such risks are generally associated with fraud and abuse, licensure, accreditation, product liability, management liability, as well as issues related to intellectual property.

TECHNOLOGY

This domain covers machines, hardware, equipment, devices and tools, but can also include techniques, systems and methods of organization. Healthcare has seen an explosion in the use of technology for clinical diagnosis and treatment, training and education, information storage and retrieval, and asset preservation. Examples also include Hospital Information System, social networking and cyber liability.

HAZARD

This ERM domain covers assets and their value. Traditionally, insurable hazard risk has related to natural exposure and business interruption. Specific risks can also include risk related to: facility management, plant age, parking (lighting, location, and security), valuables, construction/renovation, earthquakes, storms, tornadoes, foods, res.

RISK MANAGEMENT PLAN

Purpose

The purpose of the risk management program is to protect patients, staff members and visitors from inadvertent injury. The program is also designed to protect the organization's financial assets and intangibles, such as reputation and standing in the community.

The risk management plan is a primary tool for implementing the organization's overall risk management program. It is designed to provide guidance and structure for the organization's clinical and business services that drive quality patient care while fostering a safe environment.

The focus of the risk management plan is to provide an ongoing, comprehensive, and systematic approach to reducing risk exposures. Risk management activities include identifying, investigating, analyzing, and evaluating risks, followed by selecting and implementing the most appropriate methods for correcting, reducing, managing, transferring and/or eliminating them.

Authority and Role of the Risk Manager

The risk manager is empowered by the governing body to implement the functions and activities of the risk management program with the assistance of the patient care and administrative staffs. The Board of Directors has overall responsibility for the effectiveness of the program and providing the necessary resources. The Board of Director's responsibilities

are supported through regular written and verbal communications regarding risk management activities that may affect the organization's finances.

The role of the risk manager is to maintain a proactive risk management program in compliance with existing laws, rules, applicable scope of practice and regulations. The risk manager is responsible for creating, recommending to the Board, implementing, and evaluating the outcome of the risk management plan. These activities should be coordinated with quality/performance improvement, infection control, organizational/patient safety and environment of care management. The specific description of the risk manager's role may be addressed in a separate job description approved by the governing body.

The risk management program is formally addressed through designated committees, such as the risk management committee, safety committee, and quality/performance improvement committee.

Scope

Under the direction of the risk manager, the risk management program provides for collaboration among all departments, services, and patient care professionals within the organization. The risk management program provides policies, procedures and protocols to address events which may create business-related liability, professional liability, general, liability, workers' compensation, and motor vehicle liability exposures. The identification, investigation and management of accidents, injuries and other potentially compensable events are a primary responsibility under the risk management plan. This process is directed by the risk manager and others who are delegated to participate in the various components of managing adverse events occurring with patients, staff, visitors and organizational assets.

Risk management will influence, persuade and educate leaders within the following departments in order to achieve quality care in a safe environment and protect the organization's resources:

- Administration
- Allied Health and Adjunct Professional Services
- Billing Services
- Business Development and Marketing
- Clinical and Ancillary Services
- Data/Health Information and Privacy Management
- Employee Health
- Human Resources
- Infection Control
- Legal Services
- Medical Equipment
- Medical Staff
- Medical Staff Credentialing
- Patient Relations
- Quality/Performance Improvement
- Safety Management/Environment of Care
- Security Management
- Utilization Management

Objectives of the Risk Management Program

The objectives of the risk management program include, but are not limited to:

- promoting the quality of patient care, in collaboration with quality/performance improvement activities
- enhancing patient satisfaction
- minimizing the frequency and severity of adverse events
- supporting a non-punitive culture that promotes awareness and empowers staff to identify risk-related issues
- enhancing patient safety through accreditation with JCI, organizational safety strategies and other patient safety initiatives
- enhancing environmental safety for patients, visitors and staff through participation in environment of care-related activities
- utilizing risk management strategies to identify and minimize the frequency and severity of near misses, incidents and claims
- managing adverse events and injuries to minimize financial loss
- evaluating systems that can contribute to patient care, error or injury
- educating stakeholders on emerging and known risk exposures and risk reduction initiatives
- achieving requirements promulgated by accrediting organizations
- complying with state-specific scope of practice, applicable laws, regulations and standards

Specific Components

The risk management program will include the following components:

Event/Incident/Occurrence reporting

Event reporting is intended to provide a systematic, organization-wide program of reporting risk exposures to identify potential future liability. The risk management program includes an event reporting system that is used to identify, report, track, and trend patterns of events with the potential for causing adverse patient outcomes or other injuries to people, property or other assets of the organization. It is designed to reduce or ameliorate preventable injuries and property damage, and minimize the financial severity of claims.

The risk manager tracks and trends event data in order to report those findings to the quality/performance improvement department and the department(s) involved in the events for follow-up action.

Certain specific events must be reported to governmental agencies (Sentinel Events) through delineated methods. This is often a responsibility of the risk manager and compliance within established guidelines and time frames is critical.

Reporting risk management activities as part of the quality/performance improvement process

Recognizing that the effectiveness of risk management activities is contingent upon collaboration and integration with the quality/performance improvement activities, the risk manager will work with quality/performance improvement staff to coordinate activities

between the two disciplines. This will enhance the identification and resolution of risk and quality issues.

Educational activities

The risk manager will provide or facilitate orientation programs for all new employees and contracted staff. A separate annual educational program will be provided to focus awareness of risk exposures and current risk prevention activities. Other in-service and training programs should be provided as identified through the ongoing monitoring, tracking and trending of events and/or as requested by a staff member within the organization.

Management of patient and family complaints/grievances

The organization will have a formal written process for managing patient and family complaints/grievances. This process should detail response to and resolution of patient and family complaints. It should include time frames for responding, the chain-of-command used for problem-resolution, and documentation of the activities involved.

Patient satisfaction

The Patient Service will measure patient satisfaction and respond to issues identified in patient satisfaction surveys. The risk manager will monitor complaints and report findings related to quality/performance improvement. Of equal importance is risk management's direct participation in resolution of complaints, as appropriate.

Reports to the Board of Directors

The Risk Manager will provide periodic reports to the Board of Directors at least annually. The report will summarize activities, achievements, and on-going risk management issues that occurred since the prior report.

Additional or ad hoc communication shall be held with the Board of Directors for Sentinel Events, significant changes in claim reserves, claims scheduled for trial, events that may result in adverse publicity or news media attention, and severe patient injuries deemed highly likely to result in litigation.

The final annual risk management report should include all the above along with recommendations for risk control activities and identified resource needs for the coming fiscal year.

Protection of Risk Management Information Included in the Quality/Performance Improvement Program

Risk management data and information collected shall be maintained as a component of the organization's quality/performance improvement program and reported to the quality/performance improvement committee and/or designated subcommittees. This structure may result in findings being considered privileged and confidential and may be distributed outside the quality/performance improvement process only at the direction and with the written consent of legal counsel.

Review of the Risk Management Plan

The risk management plan will be reviewed, updated, and approved by the Board of Directors annually, or as needed upon recommendation by the Risk Manager.

Annual Evaluation of the Risk Management Program

The risk management program will be evaluated by the Board of Directors annually. Recommendations for enhancements are incorporated into the program prior to final approval. Financial compliance management, audit management, corporate policy and procedure management, risk management, and continuous enterprise controls monitoring.

Real-Time Monitoring and Predictive Maintenance to Prevent Incident Failure or Non-Productive Time

The upstream industry has adopted many of the same techniques to improve capital asset management. The company use a variety of techniques to reduce maintenance costs, increase uptime, and increase availability. These techniques include:

- Condition-based monitoring. Placement of sensors to measure various conditions (temperature, vibration, etc.) to detect situations that may indicate potential equipment failure. The more sophisticated systems have alerting capabilities and are integrated with enterprise asset management applications that can automatically generate inspection or work orders.

- Predictive maintenance. Predictive maintenance goes beyond condition-based maintenance in applying advanced analytics to predict potential equipment failures, providing enough notice to procure complex non-commodity replacement equipment. The algorithms identify a departure from normal operating levels of a piece of equipment rather than comparing performance with expected performance levels for the equipment class.

- Criticality-based maintenance. This technique informs decisions on maintenance strategy by identifying which assets are critical to the process and what the process impacts would be if the asset were to fail. Criticality-based maintenance also informs procurement strategy so that inventories, and the costs associated with keeping them, are reduced but not at the expense of increased downtime.

- Performance center or center of excellence. The Company intends to adopt centers of excellence where engineering staff are able to bring together engineering knowledge for root cause analysis when potential problems are identified. Centers of excellence can also have a view of multiple assets to support decision making and maintenance planning and even suggest future equipment design modifications.

Collaborative Planning, Operations and Decision Making

To reduce non-productive time, enhance production, and reduce both economic and EHS risks, the Company is creating a stronger and more comprehensive connection between field operations staff and remote experts. This connection involves:

- Collaboration. The ability for multiple parties to visualize and analyze the same set of data and information from disparate locations.

- Workflow. Rationalizing data to make it automatically available to personnel and

applications according to role-based need.

- Access to real-time data. Surface and subsurface to improve production, often involving sensors. This is often accomplished through collaboration rooms accessible from multiple locations, both on-rig and off-rig. Visualization can be 3D or 4D and, depending on the data, is most effective with a geospatial overlay.

Cyber Security Policy Design and Execution

One of the most basic elements to guarantee information security is to have an enterprise information security architecture applied to all the data, systems, processes, and people. It is imperative to be able to track from the business strategy to individual security technologies.

Information technology can help mitigate operational risks. Organizations that understand their risk profile and take concrete action to mitigate risks will be better positioned to be successful in the marketplace. It is therefore recommended that the following should be practiced:

- Consider developing a corporate wide approach to managing information in the plant. Best practices cover use of technology to support operations, business analytics, application integration, EHS compliance, and enterprise content management.

- Work to develop business processes for operations and identify document control workflow for approvals within the organization, including the transmittal and standard operating procedure (SOP) processes. Determine how often you wish to share documents with vendors, partners, regulators, and others. Work together to develop a coding standard for components/documents to ensure that there is consistent master data management.

- Participate in industry associations and user communities to help arrive at standards for sharing of content and supporting well and plant workflows.

- Look to areas of high vulnerability in your operation such as current processes that still rely on paper files that can potentially be difficult to find and update and may be misfiled or lost and ultimately expose your company to regulatory or internal audit failures.

- Focus on process improvements that will allow more effective creation and sharing of content both inside and outside the firewall. A good area to start would be the transmittal and SOP processes.

- In this time of increased regulatory pressure, look at solutions that optimize the way you manage, share, store, and archive content to comply with environmental, health, and safety regulations.

- Look at deploying information rights management tightly integrated with content management to ensure that only authorized recipients can view, copy, print, or edit confidential information.

- Reassess your customer communications capabilities to ensure timely and personalized correspondence tailored to the delivery requirements of the recipient, including customers and regulatory agencies.

- Take a more holistic approach of your asset information to ensure that drawings, records and other documentation are properly identified, stored, classified, accessible, accurate, and appropriately safeguarded.

- Familiarize yourself with emerging asset management standards such as PAS 55 and ensure that future asset management solutions that are deployed in your company operations adhere to such standards.

- Evaluate solution vendors that have the flexibility to support mobile access of project and plant information, which enables and optimizes access of information wherever it is accessed.

- Consider solutions that provide options to deploy cloud-based solutions and can support projects