Incident Management Plan

_____
Michael J. Dowling
President and CEO

_____
Mark J. Solazzo
EVP, Chief Operating Officer

_____
Eugene Tangney
SVP, Chief Administration Officer

_____
Scott Strauss
Director – Corporate EM / Security

_____
David Battinelli, MD
Chief Medical Officer

_____
Mark Jarrett, MD
SVP, Chief Quality Officer

TABLE OF REVISIONS

** This table is for the exclusive use of the System Incident Management Staff for documentation of any necessary revisions to this document.

** Furthermore, the content of this manual is subject to change without prior notice. When official revisions are made, a member of the System Incident Management Staff will complete and initial the table below. Written updates will be distributed to each facility's emergency management coordinator (EMC) for insertion into their copy of the Northwell Health System Incident Management Plan.

Revision #	Date	Section/Page(s)	Change	Updates Forwarded & Initial

System Incident Management Plan

Table of Contents

C. Situations and Assumptions

A. Hazard Vulnerability Analysis
   i. System Hazard Vulnerability Analysis
   ii. Regional Hazard Vulnerability Analysis
B. Information Technology Risk Assessment
C. Business Impact Analysis

D. Concept of Operations

A. Planning and Training
B. Mitigation
C. Incident Recognition
D. Notification
E. Response
   i. Event Activation Matrix
   ii. Emergency Classification
   iii. Emergency Response
   iv. Implementation of the Plan
F. Event Assessment

E. Incident Management

A. System Incident Command System
   i. Command
   ii. Operations
   iii. Logistics
   iv. Planning
   v. Finance/Administration
B. SICS Table of Organization
C. SICS Succession

F. Preparedness

A. Concept
B. Levels of Capability
C. Unified Approach
D. Regional Planning
E. System Planning
F. Orientation and Training
G. IMS Resources
H. Exercises and Drills
I. Special Event Planning

G. Resource Management

A. Four Primary Tasks of Resource Management
B. Concepts and Principles
   i. Concepts
   ii. Principles
      a. Advance Planning
      b. Resource Identification and Ordering

c. Categorizing Results
1). Use of Agreements
2). Effective Management of Resources
a). Acquisition Procedures
b). Management Information System
c). Ordering, Mobilization, Dispatching and Demobilization Protocols

C. Resource Availability
D. Resource Acquisition
E. Resource Allocation
F. Resource Tracking
G. Mutual Aid
H. Alternate Care Sites
I. Recovery Resources
i. Nonexpendable Resources
ii. Expendable Resources
J. Reimbursement

H. Communication and Information Management

A. Concept
B. Communication Plan
C. Crisis Management Network
D. HERDS/Commerce System
i. E-FINDS
E. Surveillance
i. Passive
ii. Active
iii. Syndromic
iv. ECLRS (Electronic Clinical Laboratory Reporting System)

I. On-going Management and Continuity of Business Operations

A. Executive Summary
B. Concept of Business Continuity
C. Business Critical Functions
D. Develop Continuity Planning
E. Staff Database and Emergency Contact Information
F. Facility
G. Hazard Vulnerability Analysis
H. Business IT Applications
I. Business Impact Analysis
J. Identify Critical Functionality
K. Application Loss Contingency Plans
L. Incident Activation Matrix
M. ICS / Direction and Control
N. Communication and Notification Plans
O. IT Disaster Recovery Departmental Procedures
P. Alternate Business Site

J. Performance Improvement

A. Concepts
B. Review and Revision of Plan
C. Evaluation Tools
D. Drills and Exercises
E. After Action Reports
F. Regulatory Compliance

K. Appendices

A. Glossary of Terms
B. EOC Telephone Contact Numbers
C. Incident Management Forms
    i. Job Action Sheets
    ii. HICS Forms
D. Hazard Vulnerability Analysis
    i. HVA Template
    ii. System YEAR HVA
    iii. Regional YEAR HVAs
    iv. Site Year HVAs
E. Hazardous Materials
    i. Hazardous Materials Plan
    ii. Hazardous Materials IRG
    iii. Radiation IRG
F. Infectious Disease Response
    i. Infectious Disease Plan
    ii. Infectious Disease IRG
    i. Point Of Dispensing POD Plan
    ii. POD IRG
G. Disaster Privileging
    i. Disaster Privileging Policy and Procedure
    ii. Disaster Volunteers Policy and Procedure
H. Fatality Management
    i. Fatality Management Plan
    ii. Fatality Management IRG
I. Severe Weather
    i. Severe Weather IRGs
        i. With Warning
        ii. Without Warning
J. Enhanced Facility Protection
    i. Enhanced Facility Protection IRG
    ii. Non-Clinical Facility Protection – Crowd Control / Public Assembly IRG
    iii. Missing Person IRG
    iv. Active Shooter IRG
    v. Utility Failure IRG
K. Evacuation / Shelter in Place / Patient Tracking

i. Evacuation/Shelter in Place/Patient Tracking Plan
ii. Planned Evacuation/Shelter in Place/Patient Tracking IRG

L. Surge Capacity and Alternate Care Sites
i. Surge Capacity and Alternate Care Site Plan
ii. Surge Capacity and Alternate Care Site IRG

M. Mass Gathering Events
i. Mass Gathering Events Plan

N. Emergency Pharmaceutical Resource Management
i. Emergency Pharmaceutical Resources
ii. New York State / DCD Chem Pack Program Description
iii. Resource List (System Availability)

O. IT Disaster Recovery Planning
i. IT Disaster Recovery Plan

P. Human Resources Planning
i. Labor Action Plan
ii. Labor Action IRG
iii. Emergency Conditions Policy

Q. Procurement Plan
i. Office of Procurement Emergency Plan
ii. Emergency Pharmaceutical Resources

R. Inventory of System Response Assets and MOUS
i. Inventory of Response Assets
ii. List of Current MOUS

S. Additional System Plans
i. Ambulatory Plans
ii. Joint Ventures Plan
iii. House Calls / Advanced Illness Management Plan

T. Partner Plans
i. New York State Burn Plan
ii. New York City Pediatric Surge Plan
iii. MACE (Mutual Aid Coordinating Entity) Operating Guidelines
iv. Nassau County Chem Pack Plan
v. Nassau County Limited Disaster Plan

U. Planning and Evaluation Tools
i. AAR Template (After Action Report Template)

NORTHWELL HEALTH SYSTEM

INCIDENT MANAGMENT PLAN

1. EXECUTIVE SUMMARY

The Northwell Health System Incident Management Plan is an outline of general policies and procedures to be followed by Health System staff when responding to an incident either within the system or within the community. This plan should be used as a guideline should an incident occur.

The Hospital Incident Command System (HICS) is utilized as a framework for incident management in all Health System entities due to its' all hazards approach to managing emergencies regardless of nature. HICS is defined by the following characteristics: a) a predictable chain of management; b) a flexible organizational chart which ensures a rapid and flexible response to emergencies; c) prioritized response checklists; d) accountability that is function specific; e) improved documentation for accountability and cost recovery; e) a common language to enhance communication with external agencies; and f) cost effective emergency planning. The System Incident Command System (NICS) is utilized by the system staff to manage incidents that have impacted or have the potential to impact one or more facilities in the system.

The goal of this plan is the effective establishment of a mechanism whereby there is assistance at the System level to any site in the Northwell Health System during an incident. The primary objective of emergency preparedness is to have the ability to mobilize and coordinate resources to meet the needs of the system and/or the community, as well as to coordinate patient care services across the continuum. This plan is intended to be universal and flexible in nature to ensure a rapid and effective response to any challenge that may result from an emergency situation. It is also intended that this incident response plan will be integrated with emergency community-wide preparedness plans to ensure a cooperative effort when necessary.

2. SYSTEM INCIDENT MANAGEMENT

a. Mission Statement

The mission of the Northwell Health System's Incident Management Program is to reduce the loss of life and property, protect our institutions from natural, technological, and man-made hazards, and preserve the system's clinical operations by leading and supporting the Health System in a comprehensive management program of mitigation, preparedness, response, and recovery.

b. Hospital Integration

Hospital integration is an important concept of the incident management program. A communication network has been established to allow a more efficient structured flow of communication during any disaster, incident, or unscheduled event. Each facility's Emergency Operations Plan (EOP) directs the facility's command staff to contact System Incident Management to aid in response, technical assistance, expertise, and direction related to an event. Furthermore, through communication with each facility's Emergency Management Coordinator (EMC), System Incident Management constantly reviews, assesses, and reevaluates all areas of concerns or improvement.

c. Regional Integration

Regional integration is the process in which the Northwell Health System, along with similar regional and local government entities, addresses all key elements in preparedness for all major emergencies and incidents. Collaboration must be established and maintained with known issues addressed prior to an event or incident. Through information sharing, participation in exercises, attendance at committee meetings, and acknowledging progress and lessons learned, true regional integration occurs.

The NIM staff is responsible for participation in regional committees for emergency preparedness, including the GNYHA Emergency Preparedness Coordinating Council, Suffolk Terrorism Task Force, and the Nassau Regional Emergency Medical Services Council (REMSCO) Disaster Committee.

d. System Incident Management Functions

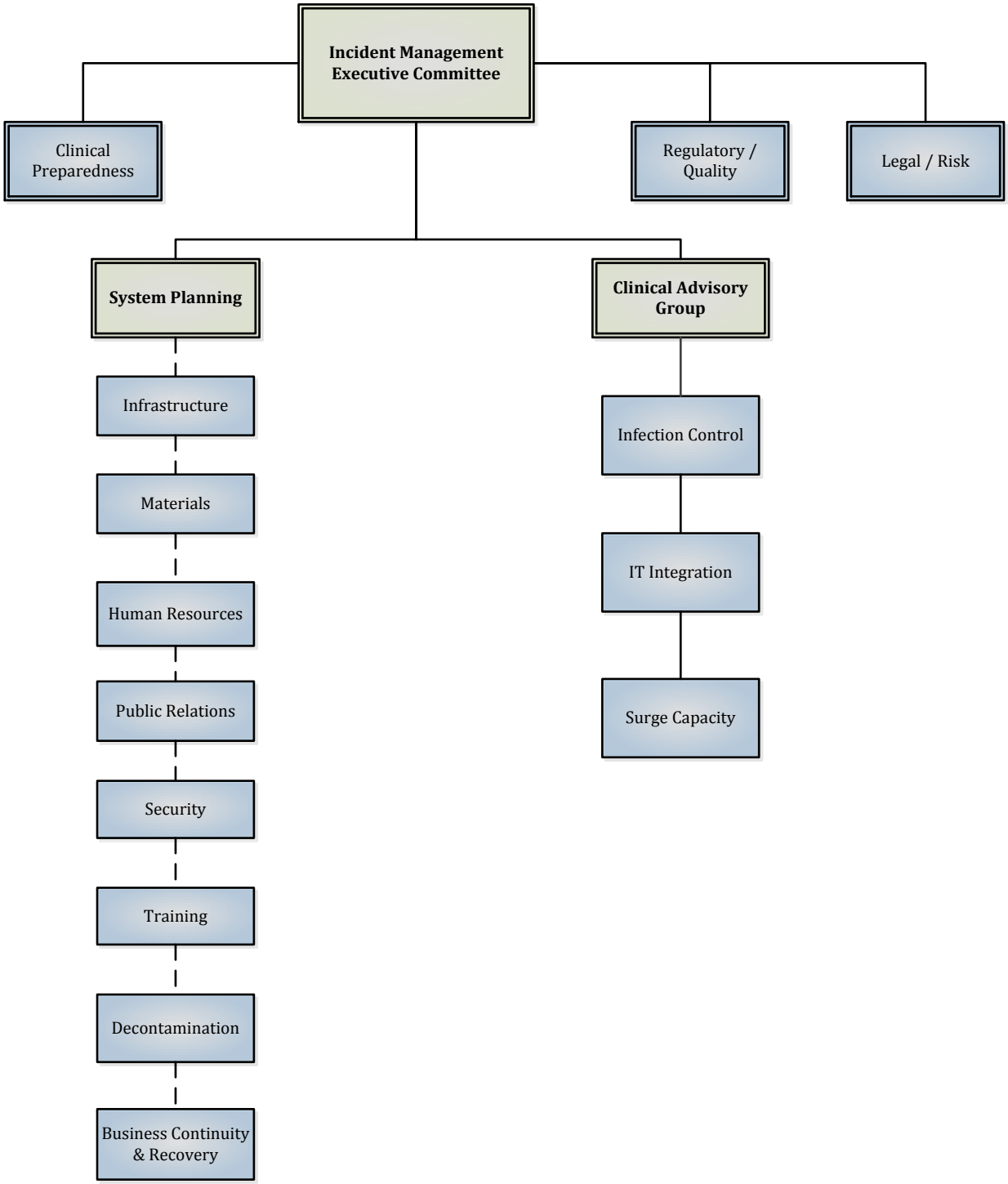
The staff of the Incident Management program provides consultation services 24 hours a day to the Health System and its' entities. These services include guidance for preparedness planning, incident mitigation, and resource availability. The Incident Management Program is structured to assist the system entities, as well as provide a well- rounded incident management platform.

e. System Incident Management Oversight and Authorities

The System Incident Management staff is comprised of a Division of the Corporate Security and Emergency Management.

The system incident management team takes its direction and works closely with the groups below to determine mitigation strategies, yearly objectives, and coordination with other system entities (i.e. Hospitals, ambulatory care / joint ventures, materials management, etc).

Exhibit A. System Incident Management Oversight Structure



f. System Incident Management Oversight Structure

The committees listed below meet as necessary to ensure that adequate and appropriate preparedness efforts and activities are taking place across the Northwell Health System. The committees serve as forums for addressing emerging issues and facilitate required collaboration when preparedness issues affect multiple entities within the system.

i. Incident Management Executive Committee

Goal: The Incident Management Executive Committee's mission is to regularly review strategy and action plans of the system's programs and committees. This committee updates senior leadership on strategy, as well as solicits input for the facility implementation strategy. *This committee has authority to develop and bypass system policies and procedures during an event or an incident.*

Attendees: *Chief Operating Officer (Chair),* Chief Administration Officer, SVP, Chief Quality Officer, Chief Medical Officer, Chief Nurse Executive, Sr. Director, Emergency Planning and Clinical Preparedness, VP, Security & Support Systems, Regional Executive Directors, and additional members as needed.

ii. Clinical Advisory Group

Goal: The Clinical Advisory Group mission is to review, update, and implement clinical practice guidelines for clinical services throughout the system as they relate to Incident and Emergency Preparedness. Provides Health System subject matter experts to help plan and prepare clinical practice guidelines for incidents, including, but not limited, public health emergencies, inter-facility care coordination, and alteration of clinical services.

Attendees: *SVP-Chief Medical Officer (Chair), SVP, Chief Quality Officer,* Medical Director, CEMS, Sr. Director, Emergency Planning and Clinical Preparedness, SVP & Chair of Emergency Medicine Service Line, VP of System Infection Prevention, Chief Nurse Executive, and additional members as needed.

Infection Control Committee

Goal: To provide health system subject matter experts to assist in ongoing surveillance and preparation for potential infectious disease outbreaks, natural or man- made. Responsibilities may include determination of isolation capacity, personal protective equipment (PPE) guidance, and curriculum development for bioterrorism and infectious disease outbreaks.

Attendees: *VP of Infection Prevention (Chair), Chief Division of Infectious Disease,* SVP/Chief Quality Officer, Medical Director, CEMS, Sr. Director, Emergency Planning and Clinical Preparedness, Medical Director of Employee Health Services, Chief Nursing Executive, AVP, Safety & Regulatory, Sr. Director, Infectious Disease, and additional members as needed.

Clinical IT Integration

Goal: To assist and provide oversight for the clinical integration of incidents and emergencies, including Electronic Medical Record modifications, as needed to maximize surveillance and patient outcomes.

Attendees: *Chief Information Officer (Chair),* Chief Medical Information Officer, SVP & Chair of Emergency Medicine Service Line, SVP, Chief Quality Officer, Chief Nurse Executive, SVP, Clinical Transformation, and additional members as needed.

Surge Capacity

Goal: To develop surge capacity activation matrices and templates for use by the Health System facilities, review best practices, identify challenges associated with surge capacity, and maintain oversight of the Special Response Team.

Attendees: *Medical Director (Chair), CEMS, Sr. Director, Emergency Planning and Clinical Preparedness,* SVP Chief Medical Officer, SVP, Chief Quality Officer, SVP & Chair of Emergency Medicine Service Line, VP of System Infection Prevention, Chief Nurse Executive, AVP, Safety & Regulatory, VP, Facility Services, Corporate Director, Security & Emergency Management, Director Patient Care Services, VP, Chief Procurement Officer, VP, Clinical Excellence & Quality, Chief Information Officer, and additional members as needed.

iii. System Planning

Infrastructure Committee

Goal: Provide a basis for maintaining and enhancing system infrastructure in the event of a defined incident. The charter of this committee includes Critical Infrastructure, Alternative Care Sites/Surge Capacity, Isolation Capabilities, Information Technology, Communications, Ambulatory Services, Joint Ventures, and Business Continuity.

Attendees: *Medical Director (Chair), CEMS, Sr. Director, Emergency Planning and Clinical Preparedness,* SVP & Chair of Emergency Medicine Service Line, VP of System Infection Prevention, SVP, Executive Director North Shore LIJ Medical Group, VP, Clinical Excellence & Quality, Corporate Director, Security & Emergency Management, VP, Facility Services, Chief Information Officer, AVP, Safety & Regulatory, VP, Chief Procurement Officer, SVP, Finance, VP, Operations Ambulatory Services, Chief Nurse Executive, and additional members as needed.

Materials Management Committee

Goal: Provide responsible material and service acquisitions, maintenance of adequate supply levels, and emergency vendor relations. This includes medical supplies, pharmaceutical supplies, food/water, housing, and other contracted services.

Attendees: *Vice President - Chief Procurement Officer (Chair),* Medical Director, CEMS, Sr. Director, Emergency Planning and Clinical Preparedness, SVP, Finance, VP of System Infection Prevention, Chief Pharmacy & Medical Safety Officer, AVP, Safety & Regulatory, Corporate Director, Security & Emergency Management, and additional members as needed.

Human Resources Committee
Goal: Develop employee related policies and guidelines for planned or unplanned incidents.
Attendees: *Senior Vice President - Chief HR Officer (Chair),* Chief Nurse Executive, Medical Director of Employee Health Services, VP, Workforce Safety, VP, Legal Affairs, SVP Chief Risk Officer, Chief Labor Officer, Chief Learning Officer, and additional members as needed.

Public Relations Committee
Goal: Develop internal and external communication strategies and social messaging related to planned and unplanned events.
Attendees: *Senior Vice President - Chief Marketing & Communications Officer (Chair), Chief Public Relations Officer*, Chief Administration Officer, SVP, Chief HR Officer, Chief Labor Officer, and additional members as needed.

Security Committee
Goal: Monitor internal and external security risks and evaluate trends and patterns of occurrences. Review of cyber terrorism policies, system lockdown procedures, and access control.
Attendees: *Vice President - Security and Support Systems (Chair),* Corporate Director, Security & Emergency Management, Site Security Directors, Chief Information Officer and additional members as needed.
.

Training Committee
Goal: To establish curriculum and training standards related to incident management, develop competencies, and facilitate the exchange of information regarding suitable training methods and materials throughout the Health System.
Attendees: *Chief Nurse Executive (Chair), Chief Learning Officer*, Medical Director, CEMS, Sr. Director, Emergency Planning and Clinical Preparedness, SVP, Chief HR Officer, Manager, Security & Emergency Training and additional members as needed.

Decontamination Committee
Goal: Standardize decontamination training and equipment throughout the Health System. This committee is also responsible for making sure the Health System is compliant with all federal regulations related to decontamination and hazardous materials spills clean-up and removal.
Attendees: *Vice President - Security and Support Systems (Chair),* VP, CEMS, Manager, Manager, Security & Emergency Training, AVP, Safety & Regulatory, VP of System Infection Prevention, Medical Director of Employee Health Services, Vice Chair Laboratory Services, Medical Director, CEMS and additional members as needed.

Business Continuity Committee

Goal: Develop a system plan for the resumption of business operations by working proactively to prevent and manage consequences of a disaster and to limit the disruption of business operations to the extent the system can afford. Elements include facility and financial recovery.

Attendees: *Chief Administration Officer (Chair),* SVP, Finance, AVP, Safety & Regulatory, VP, Facility Services, SVP, Chief Risk Officer, SVP, Executive Director North Shore LIJ Medical Group, VP, Clinical Excellence & Quality, VP, Legal Affairs, Chief Procurement Officer, SVP, Chief HR Officer, Chief Nurse Executive, Chief Information Officer, SVP, Chief Quality Officer, and additional members as needed.

g. Geography

The Northwell Health System, headquartered in Great Neck, N.Y., provides over 4 million patient contacts yearly in our catchment area, including Long Island, the Five Boroughs of NYC, and Westchester County. The system is comprised of hospitals, psychiatric facilities, hospice and home care services, a medical school, major medical research institute and many other health-related facilities in an area with a population in excess of 13 million people.

h. Incident Management Plan Organization and Revision

The Northwell Health System Incident Management staff is responsible for the maintenance of the System Incident Management Plan, its distribution, awareness, and ongoing revision, as indicated. The incident management staff will solicit updates annually from all system entities as well as copies of all hazard vulnerability assessments, risk assessments, and business impact analysis. Each year the system's Incident Management Plan will be reviewed with the system's senior leadership for their knowledge of the plan and potential systemic risks.

3. SITUATIONS AND ASSUMPTIONS

a. Hazard Vulnerability Analysis

The Hazard Vulnerability Analysis (HVA) is a way to focus attention on those hazards that are most likely to have an impact on the facility and the surrounding community. The list of hazards includes possible events or threats that may occur within the community or on hospital property. Events that impact the community are often brought into the hospital facility. It is intended that a HVA be seen as an evolving document and be reviewed at least annually within the facilities and The Joint Commission Emergency Management annual report.

i. System Hazard Vulnerability Analysis

The System Hazard Vulnerability (HVA) is a compilation of HVA data from all Northwell Health System facilities. A system-wide approach to the vulnerabilities is then expressed in the System HVA. The System Incident Management Staff will

conduct a survey of each facility on initial receipt of their HVA, allowing for confirmation that all data is correct and truly depicts their current status.

ii. Regional Hazard Vulnerability Analysis

The Community HVA is established having reviewed all community data pertaining to local, private, and governmental agency HVA's. This data is collected and reviewed with local officials to obtain a collective hazard vulnerability analysis as it pertains to that specific location. This process allows the local officials to better understand the risk and vulnerabilities of the facilities in question, and in conjunction with their pre-established community HVA's, develop a more comprehensive HVA model.

b. Information Technology Risk Assessment

Information systems have long been at some risk from malicious actions or inadvertent user errors and natural and man-made disasters. In recent years, computer based systems have become more susceptible to these threats because computers have become more interconnected and, thus, the number of individuals with computer skills is increasing, and intrusion, or "hacking", techniques are becoming more widely known via the Internet and other media.

A Risk Assessment is an essential element of risk management. However, it is only one element of a broader set of risk management tools. Other elements include establishing a central management focal point, implementing appropriate polices and related controls, promoting awareness, and monitoring and evaluating policy and control effectiveness. The risk assessment provides a basis for establishing appropriate polices and selecting cost-effective techniques to implement these polices. Since risks and threats change over time, it is important that organizations periodically reassess risks and reconsider the appropriateness and effectiveness of polices and controls they have selected.

Risk assessments, whether they pertain to information security or other types of risk, are a means of providing decision makers with information needed to understand factors that can negatively influence operations and outcomes and make informed judgments concerning the extent of actions needed to reduce risk. Regardless of the types of risk being considered, all risk assessments generally include the following elements:

- Identifying threats that could harm and, thus, adversely affect critical operations and assets. Threats include such things as intruders, criminals, disgruntled employees, terrorists, and natural disasters.
- Estimating the likelihood that such threats will materialize based on historical information and judgment of knowledgeable individuals.
- Identifying and ranking the value, sensitivity, and criticality of the operations and assets that could be affected should a threat materialize in order to determine which operations and assets are the most important.
- Estimating, for the most critical and sensitive assets and operations, the potential losses or damage that could occur if a threat materializes, including recovery costs.

- Identifying cost-effective actions to mitigate or reduce the risk. These actions can include implementing new organizational policies and procedures, as well as technical or physical controls.
- Documenting the results and developing an action plan.

c. Business Impact Analysis

Business impact analysis (BIA) is an essential component of an organization's business continuance plan. It includes an exploratory component to reveal any vulnerability and a planning component to develop strategies for minimizing risk. The end result of this analysis is a business impact analysis report, which describes the potential risks specific to the organization studied. One of the basic assumptions behind BIA is that every component of the organization is reliant upon the continued functioning of every other component, but that some are more crucial than others and require a greater allocation of funds in the wake of a disaster. For example, a business may be able to continue more or less normally if the cafeteria has to close, but would come to a complete halt if the information system crashes.

As part of a disaster recovery plan, BIA is likely to identify costs linked to failures, such as loss of cash flow, replacement of equipment, salaries paid to catch up with a backlog of work, loss of profits, and so on. A BIA report quantifies the importance of business components and suggests appropriate fund allocation for measures to protect them. The possibilities of failures are likely to be assessed in terms of their impacts on patient and employee safety, finances, legal compliance, and quality assurance. Where possible, impact is expressed monetarily for purposes of comparison.

4. CONCEPT OF OPERATIONS

a. Planning and Training

Planning and training provide the foundation for effective incident management. Plans describe how personnel, equipment, and other resources are used to support incident management and emergency response activities. Plans provide mechanisms and systems for setting priorities, integrating multiple hospitals and functions, and ensuring that communications and other systems are available and integrated in support of a full system response.

The Northwell Health System’s planning process begins with accurate risk and hazard identification. Once these indicators have been identified, the System Incident Management staff is tasked with developing plans to proactively mitigate a potential situation and develop training programs to properly educate the system staff to manage a potential incident. The System Incident Management staff provides training in hazardous materials, incident command, weapons of mass destruction and other courses to aid each system entity in their incident management skills.

Once an incident has been identified or communicated to the System Incident Management staff, the incident planning process begins. The incident planning process may begin with the scheduling of a planned event, the identification of a credible threat,

or with the initial response to an actual or impending event. The process continues with the implementation of the formalized steps and staffing required to mitigate an event based on the written incident action plan (IAP).

b. Mitigation

Mitigation is defined as the activities designed to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of an incident. Mitigation involves ongoing actions to reduce exposure to, probability of, or potential loss from hazards. Northwell's mitigation opportunities are identified by the incident management sub-committees review of facility HVA's, lessons learned from actual events or scheduled exercises, and annual reviews of infrastructure by system facilities and engineering. Once these opportunities have been identified they are forwarded to the Critical Infrastructure Protection committee. The CIP committee is tasked with prioritizing mitigation efforts and to make recommendations to senior leadership for their capital expenditure.

c. Incident Recognition

Most incidents in the Health System will not require multiple hospitals or entity involvement. The System's Incident Management staff can be notified internally or externally of an incident.

All hospitals and other entities have been instructed to notify the Emergency Operations Center at 516-719-5000 upon the identification of an incident on their property. All facilities should call into the EOC with accurate information and key contact information regarding the incident and any resources that may be needed. Each facility has in their Emergency Operations Plan detailed event activation processes and specific examples of incident notifications.

The System Incident Management and Emergency Medical Services Communications Center monitors most regional emergency service frequencies and other medias for incident notification. The System Emergency Operations Center monitors the 800 MHz alert frequency for NYC Office of Emergency Management and Nassau County Office of Emergency Management. Frequently, local emergency services agencies will contact the System EOC to notify the system of an active incident or potential for impact to the system. When this occurs, the System EOC notifies the appropriate facility that has the potential to be impacted.

d. Notification

The System Emergency Operations Center can be notified by calling the central Communication Center at (516) 719-5000. The dispatcher will ask the following questions to verify the disaster:

- Who is calling? Name and Title?
- What is their contact phone number?
- What is the location of the emergency?
- What type of emergency?
- What HICS level are they operating?

- Where is the emergency operation center?
- What is the phone number of the emergency operation center?
- What areas are affected?
- What actions have been taken by the facility?
- Are you planning for evacuation?
- What resources do you need immediately?
- Has the local municipality been notified? And if so, who and are they on the scene?

The dispatcher will have the System's Incident Management Response Notification Worksheet available outlining the necessary information needed for the appropriate response and whom should be alerted regarding this incident. The dispatcher will then activate the System's Incident Management Plan by notifying the corresponding on duty and on call incident management staff using the notification software. Each notification will list the location, level and extent of the emergency. Each member will be required to acknowledge the notification. If the on-call member of the team does not respond within ten minutes of the notification, the notification will be re-sent. The on-call Incident Management Team member will contact the original caller and make a determination of next steps to help mitigate the incident.

Notification of Local Municipalities:

New York City

New York City Emergency Management (NYCEM) will be notified upon the discretion of the System Incident Commander. The contact number is available 24 hours a day, 7 days a week:
(718) 422-8700.

Nassau County

The Nassau County Office of Emergency Management will be notified upon the discretion of the System Incident Commander. The contact number is available 24 hours a days, 7 days a week:
(516) 573-0636.

Suffolk County

The Suffolk County Fire, Rescue, and Emergency Services (FRES) will be notified upon the discretion of the System Incident Commander. The contact number is available 24 hours a day, 7 days a week:
(631) 852-4900.

Westchester County

The Westchester County Office of Emergency Management will be notified upon the discretion of the System Incident Commander. The contact number is available 24 hours a day, 7 days a week:
(914) 864-5450

e. Response

Upon activation of the System Incident Management Plan, the initial Incident Commander will make the following immediate decisions:

- Activate the incident management plan
- What immediate resources need to be sent to evaluate the situation (System Liaison, EMS resources, Haz Mat, etc.)
- Determine the classification of the disaster (Level I, II, III, IV)
- Determine the system facilities that require notification
- Establish the System Emergency Operations Center (EOC)
- Mobilize and coordinate the required resources (material and human resources)
- Coordinate patient care services across the continuum

The response decisions made by the initial Incident Commander can be modified once the System Administrator on-duty member from Incident Management is contacted.

i. Event Activation Matrix

The system has standardized the HICS activation matrix throughout the facilities for standardization of response. A copy of this matrix can be found in Appendix 3.

ii. Incident Classification

A level will be assigned to the incident based on the availability of resources. The level classification is as follows:

Classification	Impact on System	Action
Level I	Manageable with existing resources	Incident Commander notified and on stand-by
Level II	Local or site resources taxed	System Incident Management Plan Activated. Appropriate Municipalities notified
Level III	Multiple site resources exceeded	System Incident Management Plan Activated. Appropriate Municipalities notified
Level IV	System resources exceeded	System Incident Management Plan Activated. Appropriate Municipalities notified

iii. Emergency Response

When a Northwell Health System facility activates their emergency operations plan, the decision to activate the System Incident Management Plan will be made by the System Incident Management Team Administrator on-call person.

iv. Implementation of the Plan

The site emergency operations center will be established at the site involved unless conditions dictate it be relocated. A representative from the System Incident Management Team will report to the site emergency operations center.

f. Event Assessment

The incident/event will be assessed by the site Incident Commander and the System Incident Management Team representative. Appropriate HICS level will be determined and communicated as per normal procedures.

5. INCIDENT MANAGEMENT

a. System Incident Command System

The principal objectives of the network emergency incident command system are based on five major functions: Command, Operations, Logistics, Planning, and Finance/Administration.

Command represents the overall leadership organization and direction of the incident response. The remaining four functions comprise the range of activities that must be considered and/or carried out as support response to a crisis.

i. Command

The Command function serves to lead and direct the overall network mobilization and response to an emergency. This function bears responsibility for ensuring that the entire emergency response is carried out in an effective, coordinated, and efficient manner.

There are three primary staff activities that are carried out as part of the command function. They are Safety, Security, Public Information, and Liaison.

The Safety and Security functions include monitoring, and having authority over, the safety of emergency operations and hazardous conditions. In addition, these functions include organizing and enforcing facility protection and security, and traffic control.

The Public Information task entails representing the Health System as a whole while providing information to the news media.

As a Liaison, the Command function will coordinate external/internal communications with other agencies and outside facilities.

The Clinical Advisory Group is activated to serve as the Command level interface with system clinical services and provide strategic, system-wide clinical leadership.

The System Incident Commander may appoint one or more Technical Advisors to assist Command Group strategic discussion and provide subject matter expertise.

ii. Operations

The Operations function serves to organize and direct all activities relating to the System's primary mission of providing clinical care for all patients. If needed, the operations function can encompasses a number of major sub-functions depending on the operational response needs presented by the incident. Operations Branches can include: Clinician Services, Security, Facility, Business Continuity, Medical Ancillary Services, Transfer Services, Psychological Services, Patient Family Assistance and others as required.

The Clinical Services function organizes and assists with the facilitation of the overall delivery of medical care, where necessary, within the network. This includes both in-patient care, continuity of care during transportation, and triage and treatment of incoming casualties from an emergency.

The Security Branch works with the System Security Officer to assess and support security related response efforts across the Northwell Health System.

The Facility Branch focuses on maintaining the continued operational integrity of the physical plant. They include the provision of adequate environmental controls to carry out the medical mission. Facility relocation and establishment of alternate or adjunct care locations would be included under this function.

The Business Continuity Branch organizes and leads System business continuity efforts.

The Medical Ancillary Services function encompasses the organization and management of supporting resources including laboratories, pharmacy, radiology, and respiratory therapy. This function establishes responsibility to assist in the facilitation for providing optimal functioning of these services, while monitoring the utilization of necessary resources.

The Transfer Services function is responsible for support of out of service resources, transportation of personnel, supplies, food, and equipment. Duties include fueling, service, maintenance, and repair of vehicles and other ground support equipment during incidents.

The division of Psychological Support Services assures the provision of psychological, spiritual, and emotional support to staff, departments, and guests. This will also entail the initiation of the Critical Stress Debriefing Team's (CSDT) process.

iii. Logistics

The Logistics function organizes and directs those resources and activities associated with maintenance of a network physical plant, as well as the provision of adequate levels of food, shelter, and supplies to support the system's medical objectives. Logistics functions include five major sub-functions: Communications, Information Technology and Materials Supply.

The Communication function organizes and coordinates internal and external communications from the system facilities.

The Information Technology function serves to organize and coordinate all of the internal and external IT concerns. This includes the assessment of the current status of all software applications used at facilities across the system to ensure the functional capability of the System.

The Materials Supply function focuses on organizing and supplying medical and non-medical care equipment and supplies, as necessary, to support the facilities' operation.

iv. Planning

The Planning functions consolidate the management and distribution of critical information and data regarding the event, in support of the Command function. Activities include the compilation of event and resource projections encompassing the other functions, developing long-range plans for managing the event, and documenting and distributing the network's interim plans for the incident. Planning functions encompass five sub-functions: Quality Management, Situation Status, Resource Status, Patient Tracking and Labor Pool.

Quality Management functions include the organization and direction of QM related issues that concern patient care delivery and safety. This also entails the completion of failure mode analysis for incidents that possess the ability to interrupt the delivery of quality care and propose corrective actions.

Situation Status functions include maintaining current information regarding the incident status for all hospital staff, keeping a written record of the system's emergency planning and response activities.

Resource Status functions include advisement on specific capabilities, limitations of certain specialized equipment response resources. Recommend strategies for use of these resources, respond to requests for information about limitations and capabilities, and aid in the development of an action plan.

The Demobilization function drafts the Demobilization Plan with input from Command and General staff. This function also monitors implementation of the Demobilization Plan.

Patient Tracking functions encompass the organization and coordination of patient tracking and patient information. Provide documentation not limited to: patent departure/arrival times, location, and disposition.

v. Finance/Administration

The Finance and Administration functions monitor the utilization of financial assets in support of the emergency operation, as well as the related documentation necessary for managing system record keeping and reimbursement. Finance and Administration functions include four sub-functions: Procurement, Human Resources, and Claims and Costs.

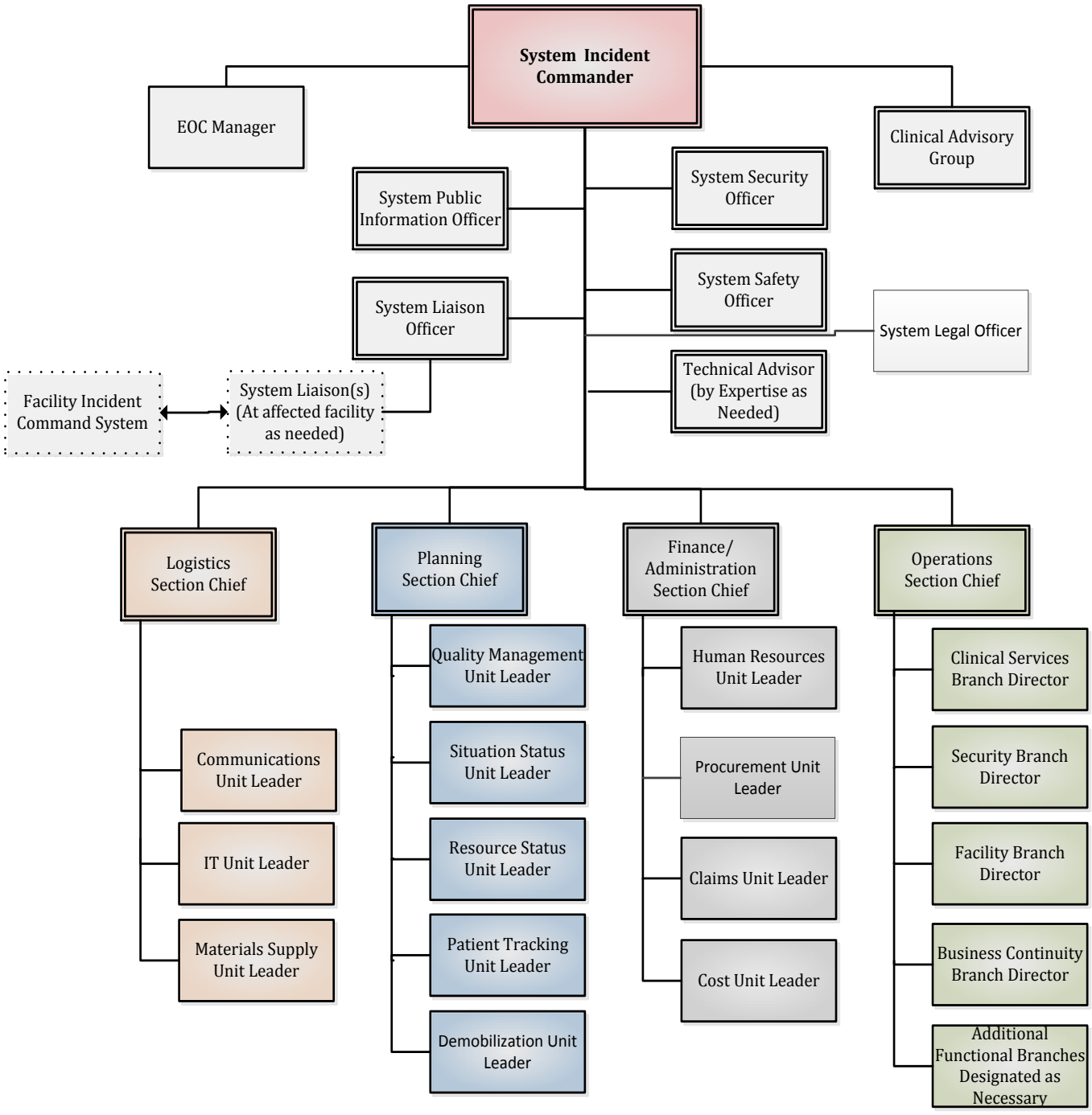
The Human Resources function includes assisting in the collection and inventory of available staff and volunteers, coordination of requests for staff support, and provision of assignments, scheduling and maintaining sufficient staffing levels.

The Procurement function encompasses the management of the acquisition of supplies and services necessary to carry out the network's mission. This function also supervises the documentation of expenditures relevant to the emergency incident.

The Claims function is responsible for receiving, investigating, and documenting all claims reported to the System during the emergency incident.

The Cost function is responsible for providing cost analysis projections and data for the incident and the maintenance of accurate records of incident costs.

b. SICS Table of Organization



This chart is not exclusive. Additional Command Staff and Branch Directors / Unit Leaders are designated functionally or geographically as needed based on the impacts of the incident.

C. SICS SUCCESSION

SICS Positions – Order of Succession Worksheet

For each position that may be activated in the Table of Organization, three (3) tiers of succession have been provided. While the "first tier" staffing is considered optimal, providing an ADDITIONAL TIER assures that each position can be staffed, if needed, at any time utilizing managerial or supervisory staff on duty in the facility. The system incident commander always retains the option of assigning staff based on assessment of the needs and Objectives to be met and availability of personnel as needed. SICS is activated by System Incident Management Staff, many of the initial SICS staff positions will be filled by the system incident management staff. The below table is a recommendation, but is subject to change by type of event, severity of event, and availability of staff.

Position	First Tier	Second Tier	Third Tier
System Incident Commander	EVP & Chief Operating Officer	SVP/Chief Admin Officer	Regional Executive Director
System Public Information Officer	Chief Public Relations Officer	AVP Public Relations	On-Call Corporate Public Relations Staff
System Security Officer	Corporate Director of Security and Emergency Management	Investigations Manager, Corporate Security	Investigator, Corporate Security
System Safety Officer	AVP Safety & Regulatory	Corporate Safety Officer	Assistant Corporate Safety Officer
System Liaison Officer	Sr. Director Emergency Planning & Clinical Preparedness	System Emergency Preparedness Coordinator	System Emergency Preparedness Coordinator
System Liaison at Affected Facility	System Emergency Preparedness Coordinator	System Emergency Preparedness Coordinator	System Emergency Preparedness Coordinator
System Legal Officer	SVP & Chief Legal Officer	On-call Legal Staff	On-call Legal Staff
EOC Manager	Administrative Manager Corp Security & EM	Executive Assistant Corp Security & EM	CLI Staff
Clinical Advisory Group	SVP, Chief Medical Officer / Group	EVP/ Physician-in-Chief / Group	SVP Medical Affairs
Technical Advisor	TBD by Incident	TBD by Incident	TBD by Incident
Logistics Section Chief	Chief Procurement Officer	AVP System Materials Management & Logistics	Director, Contracts
Communications Unit Leader	Director, System Telecommunications	Associate Telehealth Collab Tech	System Telecommunications
Information Technology Unit Leader	SVP/Chief Information Officer	VP & Chief Technology Officer	AVP, Infrastructure & Tech Management

Materials Supply Unit Leader	System Procurement Staff	System Procurement Staff	System Procurement Staff
Planning Section Chief	VP, Security & Support Systems	Manager, Emergency Management Ops	System Incident Management Staff
Quality Management Unit Leader	SVP, Chief Quality Officer	VP, Clinical Excellence & Quality	System Quality Management Staff
Situation Status Unit Leader	Sr. Director Operations	Director, System Operations	AVP, Operations SPMO
Resource Status Unit Leader	System Incident Management Staff	System Incident Management Staff	System Incident Management Staff
Patient Tracking Unit Leader	Chief Learning Officer	Medical Director CEMS	System Incident Management Staff
Demobilization Unit Leader	SVP Clinical Strategy & Development	SVP Medical Affairs	SVP, Population Health Management
Finance / Administration Section Chief	SVP, Finance	SVP, Finance	VP, Finance
Human Resources Unit Leader	SVP, Chief People Officer	Chief People Innovation Officer	AVP, HR Innovation & Org Efficiency
Procurement Unit Leader	VP, Chief Procurement Officer	AVP, System Materials Management & Logistics	Director System Materials Management
Claims Unit Leader	SVP, Chief Risk Officer	VP, Risk Management	Risk Management Staff
Cost Unit Leader	VP, Finance	SVP, Finance	Senior Manager, Finance
Operations Section Chief	SVP/ Chief Admin Officer	Regional Executive Director	Regional Executive Director
Clinical Services Branch Director	SVP, Chief Nurse Executive	Corporate Director, Nursing Operations	Office of Chief Nursing Executive Staff
Security Branch Director	Corporate Director of Security and Emergency Management	Investigations Manager, Corporate Security	Investigator, Corporate Security
Facility Branch Director	VP, Real Estate Services	VP, Real Estate Services	Director, Engineering & Infrastructure
Business Continuity Branch Director	SVP, Consolidated Services	TBD	TBD
Medical Ancillary Services	Clinical Advisory Committee	Clinical Advisory Committee	Clinical Advisory Committee

Psychological Support	Behavioral Health Response Team Staff	Behavioral Health Response Team Staff	Behavioral Health Response Team Staff
Transfer Services	Vice President CEMS	AVP CEMS Operations	CEMS Director of Operations
Transportation Officer	CEMS Operations Officer	CEMS Operations Officer	CEMS Operations Officer

6. PREPAREDNESS

a. Concepts of Preparedness

Preparedness involves:

- The development and regular testing of warning systems, response procedures, and plans for evacuation or other measures to be taken during a disaster alert period to minimize the potential loss of life and property
- The education and training of Health System leadership and employees in site and system preparedness and response
- The establishment of policies, procedures, standards, and operational plans to be applied during the disaster and following the disaster impact
- The securing of resources including the stockpiling of equipment and supplies for disaster response
- The training of specialized response teams
- The education of all system employees on how to better prepare themselves, their homes and families for an emergency/incident.

b. Levels of Capability

Preparedness involves actions to establish and sustain prescribed levels of capability necessary to execute a full range of incident management operations.

Preparedness is implemented through a continuous cycle of planning, training, equipping, exercising, evaluating, and mitigating. The Health System's all-hazards preparedness focuses on the establishment of guidelines, protocols, procedures, and standards for planning, training, personnel qualification, certification, and competency, the securing of resources, the exercising and evaluation of plans, and the utilization of mitigation activities.

Levels of capability of a facility within the Health System will be determined using the national typing protocol for the inventorying and managing of resources as described in the National Incident Management System (NIMS).

c. Unified Approach

Preparedness requires a unified approach. It is the Health System's objective to ensure that mission integration and interoperability occurs not just within the Health System, but also across functional and jurisdictional lines between our response partners, including private and public organizations, during the response to an emergent crisis or incident. Disaster response begins locally at a system level. All facility Incident Commanders will manage the incident at their facility

and will provide frequent updates of the situation to the System Incident Management Command staff. The System Incident Commander will manage the incident on a system level. In the event of a regional incident, the System Incident Management staff will provide frequent updates of the system's status to the appropriate hospital representative in the region's multi-agency coordination center (MACC). In the event of a state-wide incident, the system's status would be relayed from the MACC to the New York State Department of Health.

d. Regional Planning

The Northwell Health System participates in regional planning in all areas in which it operates through the various municipal Emergency Management Offices. The health System also works in cooperation with the various Departments of Health, first responders, Medical Examiners and all law enforcement entities.

e. System Planning

The Northwell Health System's System Incident Management Team is responsible for coordinating all preparedness activities among the system entities. They are also responsible for the coordination among non-system entities including local, state and federal agencies and public and private organizations. System Incident Management's responsibilities include developing and coordinating emergency plans, setting priorities for resources, reviewing plans and procedures, and meeting with outside entities to coordinate plans, training, exercises, and other preparedness activities.

f. Orientation and Training

Every new employee is introduced to the system's Incident Management Program on their first day of employment. This includes the key concepts of the incident command system as well as the employee's role in incident response. Additional training and education is provided throughout their employment on all aspects of the system's plan including operational procedures, use of supporting technologies, and incident recognition.

g. IMS Resources

The Northwell Health System utilizes the national typing protocol for the inventorying and managing of resources to promote common interoperability and integration as described in the National Incident Management System (NIMS). Using the NIMS resource typing protocol, resources are described using category, kind, components, metrics, and type data.

A resource is defined as personnel, teams, facilities, supplies, and major equipment available for assignment to or use during incidents. Such resources may be used in tactical support or supervisory capacities at an incident site or Emergency Operations Center.

A category is the function for which a resource would be most useful. The categories used include transportation, communications, public works and

engineering, firefighting, information and planning, law enforcement and security, mass care, resource management, health and medical, search and rescue, hazardous materials response, food and water, energy, public information, animals and agricultural issues, and volunteers and donations.

Kind refers to broad classes that characterize resources such as teams, personnel, equipment, supplies, and vehicles.

Resources can comprise multiple components. For example, the system HazMat Response Team consists of trained personnel and a comprehensive equipment cache.

Metrics are measurement standards for resources in Emergency Management. Metrics identify capability and/or capacity.

Type refers to the level of resource capability. The type assigned to a resource or component is based on a minimal level of capability described by the identified metric for that resource as defined by NIMS.

h. Exercises

Each site will conduct a minimum of two exercises per year. These coordinated efforts will be done in collaboration with the local municipalities and with response partners in private and public organizations. Exercises will be as realistic as possible and will include multidisciplinary and multijurisdictional events to test integration and interoperability. Exercise critiques will also be a joint effort between the Northwell Health System and the appropriate local municipality. The Systems Incident Management Staffs' notification procedures are tested regularly.

i. Special Event Planning

In accordance with Homeland Security Presidential Directive (HSPD) -5, Management of Domestics Incidents, all special events planning will follow the recommended guidelines established in the National Incident Management System (NIMS). This framework will provide interoperability and compatibility with each of the emergency response agencies operating or involved in the event.

7. RESOURCE MANAGEMENT

Resource management involves coordinating and overseeing the applications of tools, processes, and systems that provide the incident management team with timely and appropriate resources during an incident. The Health System's Integrated Distribution Center Plan outlines the system's procurement and distribution strategy for emergencies and disasters. Resource management shall include personnel, facilities, equipment and supplies. Resource management for the Health System shall take place within the EOC.

a. Resource management shall involve four primary tasks:

- Establishing systems for describing, inventorying, requesting and establishing resources

- Activating these systems prior to and during an incident

- Dispatching resources prior to and during an incident

- Deactivating or recalling resources during or after an incident

The concept of resource management is to effectively and efficiently respond to the resource needs of the incident. The use of standardized procedures, methodologies, and functions involved in these processes will ensure that resources move quickly.

b. Concepts and Principles:

i. Concepts: The underlying concepts of resource management are:

- To provide a uniform method of identifying, acquiring, allocating, and tracking resources.

- To provide effective mutual-aid and donor assistance and is enabled by standardized classifications of kind and types of resources required to support the incident management organization.

- It uses a credentialing system tied to uniform training and certification standards to ensure that requested personnel resources are successfully integrated into the ongoing incident operations.

- Its coordination is the responsibility of the network EOC as well as specific elements of the ICS structure.

- It shall encompass resources contributed by private sector and nongovernmental organizations.

ii. Principles: Five key principles of effective resource management:

a. Advance Planning

System Incident Management shall work in advance of an incident to develop plans for managing and employing resources in a variety of possible emergency circumstances.

b. Resource Identification and Ordering

Resource managers shall use standardized processes and methodologies to order, identify, mobilize, dispatch, and track the resources required to support incident management activities. Resource managers shall perform these tasks at the request of the IC or in accordance with planning requirements.

c. Categorizing Resources

Resources shall be categorized by size, capacity, skill, and other characteristics. This makes the resources ordering and dispatch process within the Health System, non- system entities, and governmental agencies more efficient and ensures the facility receives resources appropriate to its needs.

1. Use of Agreements

Pre-incident agreements among all parties providing or requesting resources shall be established to enable effective and efficient resource management during incident operations. Formal pre-incident agreements between system and non-system entities, including governmental agencies that might provide or request resources shall be established to ensure the employment of standardized, interoperable equipment, and other incident resources during incident operations.

2. Effective Management of Resources

Resource managers shall use validated practices to perform key resource managements tasks systematically and efficiently, including the following:

a. Acquisition procedures: Used to obtain resources to support operational requirements. System Emergency Management shall develop tools and related standardized processes to support acquisition activities including mission tasking, contracting, drawing from existing stock, and making purchases with the assistance of the Health System's Procurement Department.

b. Management Information System: A Management Information System shall be utilized to collect, update, and process data; tracking resources; and displaying their readiness status. This shall include geographical information (GIS information if available), resource tracking systems, transportation tracking systems, inventory management system, and reporting systems.

c. Ordering, Mobilization, Dispatching, and Demobilization Protocols: Shall be utilized to request resources, prioritize requests, activate and dispatch resources to incidents, and return resources to normal status. System Emergency Management shall develop standard protocols for use within the health system including, tracking systems that identify the location and status of mobilized or dispatched resources, and procedures to demobilize resources and return them to original locations and status.

c. Resource Availability:
Resource managers shall identify, refine, and validate resource availability throughout the incident life cycle. This process shall include accurately identifying (1) who is requesting resources, (2) what and how much is needed, (3) where and when it is needed, and (4) who will be receiving or using it. Resource availability within the Health System shall be coordinated with Materials Support. The management of personnel such as emergency credentialed personnel or volunteers will be coordinated by the Resource Branch Director. The Resource Branch Director shall provide the IC with all information relative to the availability of resources.

d. Resource Acquisition:
Acquisitioning of resources shall be coordinated through the System EOC throughout the duration of the incident. System EOC will coordinate requests with system Procurement, system entities, non-system entities, and governmental agencies. All acquisition relative to the operation of the incident shall be made by resource managers assigned to SIM / EOC. The Resource Manager shall provide the IC with all information relative to the acquisition of resources.

e. Resource Allocation:
The Resource Management assigned to the System EOC shall coordinate the allocation of all resources, relative to operation of the incident throughout its duration. This will include allocation of all materials and/or personnel. The Resource Managers shall prioritize allocation of resources based on the needs of the IC. The Resource Manager shall provide the IC with all information relative to the allocation of resources.

f. Resource Tracking:
The Resource Manager assigned to System EOC shall be responsible for tracking all resource throughout the life cycle of the incident. This shall include location, type, quantity and intended consignment. It shall also include security of all supplies and equipment. The resource manager must also make necessary arrangements to receive, inventory, account, audit, distribute, and reconcile all resources. The Resource Manager shall provide the IC with all information relative to the tracking of resources.

g. Mutual Aid:
The use of Mutual Aid resources shall be coordinated with the IC. The Resource Management will utilize pre-arranged agreements for specific types of request for mutual aid. If no pre-arranged agreement for a specific request exists the IC shall be consulted as to what actions should be taken to fulfill the request.

h. Alternate Care Sites:
The Resource Manager shall coordinate the use of Alternate Care Sites with the IC. The Resource Managers shall assess the availability / capability of an alternate care site for as any of the following:

- Casualty Collection Point
- Point of Distribution (POD)
- Personnel Collection Point.
- Triage area
- Temporary Morgue

i. Recovery of Resources:
The Resource Manager shall be responsible for the recovery and final disposition of all resources utilized throughout the incident's life cycle. This shall include the restocking, replenishing, rehabilitation, and disposal of all resources.

i. Nonexpendable Resources:
A full accounting for all nonexpendable supplies and equipment shall be made during the recovery phase of operations. All nonexpendable supplies and equipment shall be returned to their point of issuances. All equipment shall be fully functional and made ready for next deployment. Any lost or broken equipment shall be noted or marked accordingly.

All personnel shall be afforded adequate rest and rehabilitation prior to demobilization. Important occupational health and mental health issues must be addressed, including monitoring the effect of the incident on personnel over time.

ii. Expendable Resources
A full accounting of all expendable resources consumed during the duration of the operation shall be completed during the recovery phase. Restocking of all spent items shall be completed. Waste management for the disposal of any perishable, biological, or contaminated objects, as well as other debris and equipment shall be handled accordingly.

j. Reimbursement:
Reimbursement for expense incurred during the operation of an incident shall be coordinated with the Finance / Administration Section of the IMS. The Northwell Integrated Distribution Center Emergency Plan outlines System procurement processes which have been designed to provide necessary documentation to support reimbursement efforts.

8. COMMUNICATION AND INFORMATION MANAGEMENT

a. Concept
The principal goal of communication and information management is to establish and maintain a common operating platform and to ensure accessibility and interoperability. These includes providing a framework to formulate and disseminate indications and warnings, formulate, execute, and communicate operational decisions and needs at an incident site, as well as between incident management entities across jurisdictions and functional agencies.

A common operating system allows incident managers at all levels to make effective, consistent, and timely decisions. Integrated systems for communications, information management, and intelligence and information sharing allow data to be continuously updated during an incident, providing a common framework that covers the incident's life cycle across jurisdictions and disciplines.

b. Communications Plan

The Northwell Health System Emergency Operations Center is open and staffed twenty-four hours a day and can be contacted during business hours at 516-719-5100. The staff from the Center for Emergency Medical Services (CEMS) Communications Division provides support to the system incident management staff as controllers to receive any and all incident management activations or notifications. The primary call number for the EOC is (516) or (631) 719-5000.

Each staff member of System Incident Management has been issued a Smartphone, WiFi Hotspot, and IPad for business purposes. In addition, the Incident Management division maintains 12 spare Nextel phones, and has the ability to utilize satellite phones in the event of an emergency. These units are maintained by the incident management staff and can be dispatched to any system entity during a communications failure.

The System EOC utilizes Cablevision Lite Path has its primary phone service. The PBX is on UPS battery back-up and is wired to our generator. The System EOC also maintains a standalone Verizon PBX on the 496 exchange. These numbers are published in the Communications appendix for reference. In the event of a telephone failure, the Verizon system will be utilized immediately. All system facilities' telecommunications staff will be notified of the temporary change.

Each system hospital maintains a communication plan in their Emergency Operations Plan (EOP). Each hospital has a primary phone system and a back-up phone system usually designated as their "red phone". Each system has their redundant phone system numbers published in their EOP. The System EOC also has a VSAT (Very Small Aperture Terminal) communications system, which allows for data and voice transfer (via satellite) between facilities in the event of a communications failure, and satellite phones.

The System EOC maintains multiple e-mail addresses to receive information from internal or external sources. The primary e-mail address for the EOC is EmergencyManagement@northwell.edu. In the event of a failure of the Network Internet connectivity or the Network Infrastructure, the EOC uses nslijemergencymanagement@gmail.com. In addition, the Health System maintains a Twitter account (@NSLIJCSNEM) and a Facebook account (Northwell Health System Emergency Management).

In the event of a telecommunications failure at any specific site, the entity can contact System Incident Management on the Mutualink System via each site's security radio system. Once this notification has been made to the EOC, System Incident Management will be notified of the need for resources to be dispatched to the impacted facility.

The Northwell Health System Incident Management staff regularly communicate via the system's conventional UHF trunked radio system. This system utilizes Motorola's One Voice System, which is a Radio over IP (ROIP) operational platform. The ROIP transmitters are maintained by a partnership between Motorola Communications and Integrated Wireless Technologies, with each site having its own battery back-up and generator power.

Incident Management maintains an Analog UHF point to point radio frequency in the event of a complete network failure. All Nassau County and New York City system hospitals, as well as the System EOC, have access to 800MHz radios to communicate with their respective local municipal Emergency Management offices.

In addition, The Northwell Health System has deployed a Mutualink Interoperability System, in which all hospitals utilizing their security operations radio have direct communications to System Incident Management. The Mutualink System allows for outside agencies, such as local law enforcement, fire, and EMS, to have seamless voice, data, and multimedia communications with each of our facilities and the System EOC. The system is built with a double redundancy utilizing two independent internet providers with additional failover to intranet in the event of a multiple carrier outage. The system can also be ported to satellite or cellular data networks in the event of complete network failure.

Amateur Radio (HAM) can also be utilized as a backup system for radio communications. By utilizing dynamics of radio waves and tuning radio communications with HAM, the radio can travel long distances without repeaters and are capable of functioning with minimal power and infrastructure requirements. The Health System has licensed HAM operators at multiple sites including the System EOC. Some hospitals have purchased, or received from a grant, HAM radio equipment. In the event that additional licensed HAM operators are needed, partnerships have been forged with the local ARES and RACES groups.

c. ETEAM Incident Management Software

The Northwell Health System utilizes ETEAM, a web-based incident management software program. ETEAM provides the incident command staff, at the network and facility levels, the ability to send and receive alert notifications and incident updates, request and track resources, and establish action plans for the duration of the incident. With the ability to analyze and respond in real-time, ETEAM provides a platform for the incident command staff located at each facility to communicate amongst themselves, as well as with the system and other regional entities. Furthermore, the information entered by all players involved in the incident allows decision makers and emergency management personnel to sort, prioritize, and visualize the volumes of critical data that pours into a command center during an incident. ETEAM offers the following features: incident reporting and tracking, tip reporting, hazard modeling, resource management, action planning, alert notification, and ESRI-enabled geographic information systems (GIS) mapping. ETEAM also allows for data sharing with the emergency management divisions of Nassau and Suffolk Counties, providing for real-time interoperable incident communications.

d. **Mass Notification System**

The Northwell Health System has deployed Everbridge Mass Notification which enables users to send notifications to individuals or groups using lists, locations, and visual intelligence. This notification system is designed to keep leadership and employees informed before, during, and after an event. Everbridge Mass Notification software provides robust analytics, GIS targeting, flexible group management, distributed contact data, language localization, and multiple options for contact data management. The system supports over 30 different multimodal delivery methods with voice recording, text to speech conversion in multiple languages, push

notifications, rich text formatting, and SMS. Each site has several "dispatchers" who have the ability to send messages specific to localized events, while the Health System remains the owner and can send messages system-wide.

d. HERDS/Commerce System

The Health Emergency Response Data System (HERDS) was designed by the New York State Department of Health (NYSDOH) to allow health care systems throughout New York State and the NYSDOH to identify and monitor public health incidents as they occur. HERDS is used by all the hospitals in the Northwell Health System for reporting on emergency incidents and for completing hospital surveys when requested by the NYSDOH. All system facilities must have an HPN (Health Provider Network) Coordinator and the Communications Directory must be kept current. During an incident, facilities will be notified by the NYSDOH when information is required to be entered. This information may include information on patients related to the event as well as the number of needed or available beds, equipment, personnel, antibiotics, antidotes, blood products, supplies, and pharmaceuticals.

The Health Emergency Response Data System (HERDS) may be accessed via the Health Commerce system using the following website: https://commerce.health.state.ny.us/public/hcs_login.html. A user ID and password is required to gain access to this site.

e. eFINDS

The eFINDS application is the Health Commerce System (HCS) platform for sharing of patient/resident location information when facilities need to relocate their patients or residents. The application captures minimal amounts of data, and allows facilities to track the patient/resident movement to other facilities, facility types or temporary shelters. This information is shared in real time by Health Commerce System authorized users statewide, and was designed to document patient/resident location, as well as provide day to day or hourly updates as needed.

f. Surveillance

Surveillance is the ongoing, systematic collection, analysis, and interpretation of data related to a specific agent or hazard, risk factor, exposure, or health event. Surveillance is essential to the planning, implementation, and evaluation of emergency management plans, and must be closely integrated with the timely dissemination of the data to those responsible for prevention, response, and control. Surveillance is a continuous and systematic process.

Surveillance systems utilize a framework which involves goals and objectives, case definitions, data collection, data analysis, reporting and notification, feedback, and evaluation of the system. The Northwell Health System utilizes types multiple surveillance systems including passive, active, and syndromic surveillance. The Health System also reports surveillance data to the local Departments of Health and the NYS Department of Health.

i. Passive Surveillance

Passive surveillance relies on the review of medical records or occupational health records as well as reports from physicians and labs to obtain information about infectious disease cases. The data is provided but not analyzed.

ii. Active Surveillance

Active surveillance involves the review of daily laboratory culture final results, medical record reviews, computer based surveillance, the evaluation for trends and epidemics, and the timely reporting of findings. The Infection Control Departments at each facility have rigorous active surveillance systems.

iii. Syndromic Surveillance

Syndromic Surveillance is used to monitor disease trends and detect outbreaks by looking at chief complaint data from Emergency Department records, laboratory data, hospital admissions data, and pre-hospital care reports. The health system has implemented a process to identify hospital acquired infections and potential outbreaks within the community based upon the Emergency Department's chief complaint data, admissions data, and laboratory reports provided by the laboratory and System Incident Management call volume and resource requests, targeted screening for infectious diseases at points of entry as emerging diseases present, unusual infectious events that present with unknown origin, and increased in-patients trends without infectious etiology or cause for increase. Health system and facility infection prevention personnel, along with Infectious Disease physicians are notified based on the identification of the event. Discussion and validation prompts health system and facility notification of the potential disease outbreak and/or event. This enables the Health System to outline and employ an immediate response to contain the pathogenic agent.

iv. ECLRS

The NYS Department of Health has created a statewide surveillance system known as the Electronic Clinical Laboratory Reporting System (ECLRS). ECLRS was designed to be a fully automated system that allows laboratories to electronically submit files to the NYS Department of Health who would then analyze the data and use it to monitor for trends and epidemics. The North Shore-LIJ Health System's Core Laboratory and functional laboratories within the health system currently submits data to the NYS Department of Health through the ECLRS system. The Health System also electronically submits laboratory result files to the local Departments of Health (currently New York City Department of Health and Mental Hygiene) that have the technology to receive them.

g. Situational Awareness

System Incident Management personnel utilize multiple software and intelligence sources to monitor incidents locally, regionally, nationally, and internationally that may have an impact on

the Health System's ability to provide services to the populations it serves. This daily situational awareness is shared with senior leadership and the facilities on a regular basis. Information monitored by System Incident Management includes local and regional incidents involving law enforcement, fire, and EMS, weather forecasts, hurricane tracking, power outages, infectious disease outbreaks, and national and international incidents including terrorism, labor actions, and transportation incidents.

9. CONTINUITY OF BUSINESS

a. Executive Summary

The Northwell Health System has specific emergency operations plans, policies, and guidelines for implementation during incidents. The primary objective of an emergency operations plan is to enable each facility to readily identify a disaster; manage its impact to protect staff, patients and visitors while attempting to re-establish normal operations. In order to survive, each facility must assure that critical operations can resume normal processing within a reasonable timeframe of an incident or interruption of service. These critical operations must be identified prior to an incident; their impact on the health system's ability to deliver quality care, effectively and safely to our patients must be analyzed and proactive solutions to harden these systems must be recommended.

Historically, the data processing function alone has been assigned the responsibility for providing business continuity and contingency planning. Frequently this has led to the development of recovery plans to restore computer resources in a manner that is not fully responsive to the needs of the business supported by these resources. Contingency planning for resumption of business operations is a "business owner" issue rather than a data processing issue.

Resumption of business operations, also called business continuity planning, is the act of proactively working out a way to prevent, if possible, and manage the consequences of a disaster, limiting it to the extent that a business can afford. An effective plan serves to secure business entities against financial disasters. The payoff for the system is maintaining quality patient care, enhanced customer satisfaction, enhanced corporate image in the eye of the public, and no dip in market share.

The goals of the resumption of business operations should be:

- Identifying weakness through annual BIA/HVA and implement prevention strategies to eliminate or lessen their impact
- Minimize the duration of disruption
- Facilitate effective co-ordination of recovery tasks
- Reduce the complexity of the recovery effort

b. Concept of Business Continuity/Continuity of Operations

The Northwell Health System's responsibility for business continuity lies at the business owner in the facilities. These independent entities have been tasked with reviewing policies, procedures,

and staff recognition of how they will perform in the event that an aspect of their infrastructure is lost.

The system's incident management staff review annually continuity plans for business owners in their review of each facilities emergency operations plan. Copies of each business owner's continuity plans specific to a specific application can be found in the entities emergency operations manual, their administrative manual, and with Information Technology.

c. Business Critical Functions

The Northwell Health System treats patients twenty-four hours a day, 365 days a year. The health system's normal business hours are when any patient is being treated in our facilities. All business applications and their corresponding technology must be able to meet the needs of these challenges and the supportive staff to run these programs must be well educated.

The Northwell Health System's incident management staff have identified critical areas of opportunity to improve emergency preparedness. The resumption of normal business operations during an interruption of service or a disaster is not limited to information technology and the financial institutions. Business resumption includes parameters surrounding:

i. Data recovery
ii. Financial functional resumption
iii. Staffing relocation
iv. Facilities and utilities
v. Communications
vi. Materials support
vii. Payroll / human resource activities
viii. Alternate operational sites

d. Develop Continuity Planning Team

The continuity planning for the Health System is a part of the Critical Infrastructure Protection structure of the system. The staff participating in the CIP committee is also free to participate in the Continuity of Operations program. As a minimum the business continuity team consists of:

i. Information technology
ii. Network Operations
iii. Facility manager
iv. Safety
v. Senior Leadership
vi. Legal / Risk management

e. Staff Database and Emergency Contact Information

The Information Technology staff of the Office of Chief Information Officer is responsible for the parameters and applications of the information network for the system. Annually, the OCIO staff reviews all mission critical applications, assess their risks, establish a key contact list for the business owner, and make recommendations for the improvement, enhancement, or replacement

of these applications. During an IT outage the OCIO staff is responsible to the notification of these business owners and the after action reporting to these owners.

f. Facility

The System Incident Management staff is responsible for the maintenance of the Emergency Operations Center. The EOC maintains records of the facility layouts of our hospitals and major real estate holdings. Each facility engineering staff is required to maintain these records on-site in their respective EOC and can utilize the System's EOC's information as redundancy and off-site storage.

i. The System Emergency Operations Center has a floor plan on hand and in offsite storage indicating the following:

   A. Utility shut-off locations
   B. Water hydrants
   C. Water main valves
   D. Water lines
   E. Gas main lines
   F. Gas valves
   G. Electrical service
   H. Electrical cutoffs
   I. Storm drains
   J. Sewer lines
   K. Alarm panel and enunciator
   L. Fire suppression systems
   M. Fire extinguishers
   N. Exits
   O. Stairways
   P. Hazardous Material storage
   Q. Elevators
   R. Standpipe connections
   S. Generator location
   T. Generator size

ii. Identify all evacuation routes and map them
iii. Have digital photographs of key assets
iv. Identify evacuation/safety team members
v. Identify evacuations and accountability plans
vi. Ensure Fire Drill compliance
vii. Identify all hardware IT / Telecom assets

g. Hazard Vulnerability Analysis

Each department will perform an annual risk assessment of their ability to complete their mission and the potential hazards that may hinder that operation. System Incident Management recommends that each business entity perform both a Hazard Vulnerability Analysis and a Business Impact analysis. These risk profiles will be reviewed with System Emergency

Management staff annually and will be used to make recommendations for mitigations strategies to coincide with available capital resources.

h. Business IT Applications

All mission critical applications are under the direct control of Information Technology, their vendor, or the independent business owner. All entities are required to maintain recovery records of their applications and their contingency plans should be exercised annually. The current list of applications is maintained in the Datacenter offices of the OCIO. Its lists:

i. List all software applications used in the entity
ii. Have all recent copies of software licensing agreements and contracts copied and placed offsite storage
iii. Identify all hardware needs per software (schematic mapping)
iv. List all PC /Laptop Names/Printers/Fax machines (IT Network #)
v. List all IP addresses of staff
vi. List all servers and Network tree locations they can identify

i. Business Impact Analysis

Business Impact Analysis is the process of identifying the critical business functions and the losses and effects if these functions are not available. It should identify:

i. All contractual agreements where you provide the service
ii. All legal responsibilities you have to your employees
iii. Quantify loss of services to your line of business and its dependents
iv. Cost analysis of software recovery
v. Impact:
    - How vital the function is to the overall business strategy
    - How long the function can be inoperative without impact or losses
    - How the rest of the business would be affected by its outage-downstream operational impact?
    - What is the revenue lost due to its outage?
    - Whether its outage would result in a violation of regulatory requirements, contractual agreements, impose penalties or whether it would create legal issues?
    - Whether it would affect relationships with customers or loss of customer confidence
    - Whether it would affect industry ranking
    - What the maximum acceptable/permissible outage would be

vi. Recovery:
    - What are the resources required to continue the function
    - Which would be the bare minimum resources needed
    - Which of these resources would be delivered from an external source

- Who is responsible for delivering computer equipment to the alternate location?
- Under which external business vendors would it be dependent?
- What is the time and effort required to recreate up to date data from back-ups

j. Identify Critical Functionality

Functionality will be classified by its impact on processes and patient services:

- *Critical* – if interrupted or unavailable for some time, it can completely jeopardize the patient services and business processes and cause heavy damage
- *Essential* – functions whose loss would seriously affect the organizations ability to effectively and safely treat patients.
- *Necessary* – the organization can continue functioning; however, the absence of the functions would limit their effectiveness to a great extent
- *Desirable* – these functions would be beneficial, however their absence would not affect the capability of the organization

The business owner with Information Technology staff should come up with standard recovery timeframes that are acceptable and realistic:

- *Critical* – less than 24 hours
- *Essential* – 2 days to 4 days
- *Necessary* – 5 days to 7 days
- *Desirable* – less than 10 days

It will also define resource requirements for making a business function operational after interruption or disaster. This includes manpower, documents, records, phones, faxes, PC's, whatever complete specifications.

k. Application Loss Contingency Plans

Each business owner is required to maintain and exercise contingency plans in the event that their application or their ability to treat a patient or provide a service has been compromised. Other than clinical requirements, each business owner should concentrate on:

- Secondary Technology (cellular modems; analog lines, laptops, paper transactions, printed timesheets)
- Critical Resources to be retrieved
- Critical Function recovery tasks
- Identify Internal Resources
- Identify External Resources

l. Incident Activation Matrix

As with the system's incident management plan, each entity should develop a matrix for activation guidance that is specific to each mission critical application for staff to follow.

m. ICS / Direction and Control

Any interruption of service or any loss of the ability to provide safe and effective care to our patients requires systemic notifications. All interruptions and disasters are managed in the North Shore – LIJ Health System by an Incident Command System. Depending on the nature and severity of interruption will determine the extent of network involvement as guided by the System Incident Management Plan.

n. Communication and Notification Plans

Information Technology has a notification process in the event of a IT network interruption. This call tree includes notification to the System Emergency Operations Center and staff. Each business owner should include in their continuity plans a communication plan and a notification process including notifications to the following:

i. System
ii. Senior Leadership
iii. Employees
iv. Team Alert List
v. Informational hotline
vi. Employee Call List Description
vii. Team Meeting Place
viii. Vendors
ix. Customers
x. Employees' families

o. IT Disaster Recovery Departmental Procedures

The OCIO of the Northwell Health System is responsible for maintaining the Disaster Recovery strategy for the system. Northwell strategies for incidents impacting business functions are detailed in the System Business Continuity Plan. These plans include the following information:

i. Business Termination / Facility Shutdown procedures
ii. Resumption strategies
iii. Records Preservation / Security
iv. Data Storage and off site Redundancy
v. Recovery Team

p. Alternate Business Site

In the event that Burke Lane or any of the system entities have lost the ability to maintain a functioning posture in their building, the System Incident Management staff is tasked with assisting Physical Assets in determining the following:

- Physical structure for long term
- Resources Required Over Time
- IT/Telecom assets needed
- Servers and network directional feed
- Office supplies
- Furniture
- Staffing schedules
- Communications capabilities
- Communicate new location to employees, customers, vendors

Physical Assets is responsible for maintaining an updated list of owned and leased space, including unoccupied space, within the Health System, along with the capabilities of each site (e.g. IT infrastructure, generator, etc….). In the event that a system entity can no longer function in their current space, arrangements will be made to move them into an unoccupied space which meets their needs.

10. PERFORMANCE IMPROVEMENT

a. Concepts

Performance Improvement is a process that assists institutions in achieving the desired outcome of providing high quality services. This is achieved through a systematic process that describes desired performance, identifies gaps between the desired and actual performance, identifies the causes of the gaps by looking at processes, selects interventions to correct gaps, and measure changes in performance.

In Emergency Management, Performance Improvement is achieved through annual review and revision of the System Incident Management Plan, use of evaluation tools to monitor and evaluate desired performance, exercises to identify gaps between the desired and actual performance, and After Action Reports to aid in the recognition of gaps and in the development of processes to meet desired outcomes.

b. Review and Revision of Plan

The Northwell Health System Incident Management staff is responsible for the maintenance of the System Incident Management Plan, its distribution, and its revision. The emergency management staff will solicit updates annually from all system entities and copies of all hazard vulnerability assessments, risk assessments, and business impact analysis. Each year the System Incident Management Plan will be reviewed with the system's senior leadership for their knowledge of the plan and its risks.

c. Evaluation Tools

Evaluation of the System Incident Management Plan requires accurate observation and careful documentation of incidents. A standardized approach helps capture the specific strengths and weaknesses of the plan and the system's response. Using standardized planning, observation and evaluation principles allows for a consistent record each time an exercise occurs within a system facility, and allows for comparison from one exercise to the next to determine if improvements

were made in areas that had been identified as weaknesses. The Northwell Health System utilizes the Homeland Security Exercise and Evaluation Program (HSEEP) when conducting exercises.

d. Exercises

System exercises will occur at least once per year. These coordinated efforts will be done in collaboration with the local municipalities (New York City, Nassau County, Suffolk County, and Westchester County) and with response partners in private and public organizations. Exercises will be as realistic as possible and will include multidisciplinary and multi-jurisdictional events to test integration and interoperability. Exercise critiques will also be a joint effort between the Northwell Health System and the appropriate local municipality. Recognizing the impact of potential regional hazards that will result in an influx of patients at all area hospitals (e.g. coastal storm evacuation, pandemic influenza, etc.), the system will participate in at least one regional exercise each year that will include an influx of actual or simulated patients (e.g. transport of paper charts).

System exercise scenarios and objectives will be based upon actual and perceived hazards identified in the System Hazard Vulnerability Analysis. Clearly defined scenarios and objectives will be written prior to the exercise and objectives will be distributed to all participants prior to the start of the exercise. Exercise design and planning will be compliant with the Homeland Security Exercise and Evaluation Program (HSEEP) principles.

Although all exercises will have unique objectives based upon the specific scenario, all exercises will be monitored to determine how well the System accomplished the following:

- Adherence to NIMS/ICS structure
- Event notification/activation
- Effectiveness of internal and external communications
- Resource management including acquisition, allocation, and tracking
- Patient management/clinical activities
- Staff roles and responsibilities

e. After Action Reports

The After Action Report (AAR) is a crucial part of the feedback system that drives improvements prevention and preparedness of the system's response to incidents. The AAR documents performance and captures strengths and weaknesses that are identified by the exercise participants, observers, and evaluators through "hot wash" discussions conducted following the exercise, written evaluations by all exercise participants including observers and evaluators, and an improvement action plan. The AAR provides a description of what happened, strengths, areas for improvement, and recommendations for corrective actions. The Improvement Action Plan (IAP), included in the AAR, provides a summary of the areas for improvement and corrective actions, as well as assigning a responsible party and timeline for completion. An AAR will be prepared for each tabletop, functional exercise, drill, and full-scale exercise conducted by each facility and the system. A copy of the site AARs will be forwarded to the System Incident Management within sixty (60) days of exercise completion.

System Incident Management will complete an AAR for all system-wide exercises and after all actual incidents in which System Incident Management personnel and/or resources were mobilized. For System activations and exercises, the System Incident Management staff is responsible to collect comments and critiques, develop the Improvement Action Plan, and to prepare the AAR. System Incident Management staff is responsible for forwarding all necessary modifications to the System Incident Management Plan to the Emergency Management Executive Committee for review.

f. Regulatory Compliance

System Incident Management addresses all standards and guidelines applicable to emergency preparedness including New York State Department of Health 405, New York State Emergency Preparedness Guidelines for Nursing Home & Extended Care Facilities, The Joint Commission Emergency Management Standards, Center for Medicare and Medicaid Services (CMS) Conditions of Participations (CoPs), the National Institute for Occupational Safety and Health (NIOSH), the Centers for Disease Control and Prevention (CDC), and the National Fire Protection Association (NFPA).