Incident Response Guide: Information Technology (IT) Failure

Mission

To provide for business continuity and availability of essential automated systems for the hospital in the event of a massive or sustained information technology failure, cybersystems compromise, or deliberate attack.

Directions

Read this entire response guide and review the Hospital Incident Management Team Activation chart.
Use this response guide as a checklist to ensure all tasks are addressed and completed.

Objectives

- ☐ Maintain patient care capabilities
- ☐ Isolate and repair affected information technology systems
- ☐ Notify affected end user supervisory personnel and provide directed guidance on information technology systems use
- ☐ Restore automated systems and services

Immediate Response (0 – 2 hours)				
Section	**Officer**	**Time**	**Action**	**Initials**
Command	**Incident Commander**		Activate the Emergency Operations Plan, Information Technology Failure Plan, Hospital Incident Management Team, and Hospital Command Center.	
			Establish operational periods, objectives, and regular briefing schedule. Consider using the Incident Action Plan Quick Start for initial documentation of the incident.	
			Consider limiting or ceasing nonessential services.	
			Notify the hospital Chief Executive Officer, Board of Directors, and other appropriate internal and external officials of situation status.	
	Public Information Officer		Prepare an initial risk communications for staff and patients regarding the cybersystems situation and recommend actions until the system is restored.	
			Update internet, intranet, and social media with the hospital's status and any alteration in services.	
			Notify key staff including house supervisors, Chief of Staff, Business Continuity Branch Director, support services, and others designated in the Business Continuity Plan as it applies to cybersystem disruptions.	
			Monitor media outlets for updates on the incident and possible impacts on the hospital. Communicate this information via regular briefings to the Section Chiefs and the Incident Commander.	
	Liaison Officer		Notify community partners in accordance with local policies and procedures (e.g., consider local Emergency Operations Center, other area hospitals, local emergency medical services, and healthcare coalition coordinator), to determine incident details, community status, and establish contacts for requesting supplies, equipment, or personnel not available in the hospital.	
			If the disruption is deliberate and targeted, contact local law enforcement, the Federal Bureau of Investigation (FBI) Cyber Division, and the state cyber terrorism division, as appropriate.	

	Safety Officer		Provide for the safety of patients, staff, and visitors in areas impacted by the automated system shutdowns.	
			Initiate the HICS 215A to assign, direct, and ensure safety actions are adhered to and completed.	

Immediate Response (0 – 2 hours)				
Section	**Branch/Unit**	**Time**	**Action**	**Initials**
Operations	**Section Chief**		Determine if personnel and resources are available to successfully complete the Operations Section strategies and tactics as outlined in the Incident Action Plan. If not, contact Logistics Section to request additional personnel or resources.	
	Medical Care Branch Director		Provide for the continuation of patient care and management activities, including the documentation of medication administration, patient care, and supply use.	
			Implement downtime patient care documentation and critical diagnostic and support systems until systems can be restored.	
	Infrastructure Branch Director		Direct an inspection of critical monitoring functions that may be affected by the incident.	
			Conduct a risk assessment of affected environmental systems (e.g., heating, ventilation, air conditioning, and utilities) and implement plans to maintain affected systems that support hospital operations.	
	Security Branch Director		Provide for security of the hospital, including manual patrols and controls of ingress and egress.	
	Business Continuity Branch Director		Work closely with the Infrastructure Branch to implement the Business Continuity Plan.	
			Assess the degree of cybersystem intrusion or disruption. Recommend any interim measures and corrective actions.	
Planning	**Section Chief**		Establish operational periods, incident objectives, and the Incident Action Plan in collaboration with the Incident Commander.	
	Situation Unit Leader		Determine the affect of system interruptions on the ability to gather and share incident information and impacts.	

	Documentation Unit Leader		Collect and collate manual documentation of the incident.	
Logistics	**Section Chief**		Refer to the Job Action Sheet for appropriate tasks.	
	Service Branch Director		Implement emergency internal communication and reporting mechanisms.	
			Isolate and repair, replace, or remove affected systems from the hospital network; establish restoration priorities in accordance with the Business Continuity Plan.	
			Provide for the integrity of system backup data and begin planning for system restoration.	
	Support Branch Director		Implement manual inventory and resupply processes, including medication distribution.	
			Coordinate the transportation services (ambulance, air medical services, and other transportation) with the Operations Section (Medical Care Branch) to ensure safe patient relocation, if necessary.	
			Obtain and distribute supplies, equipment, medications, and food and water to sustain operations.	

Intermediate/Extended Response (2 to greater than 12 hours)				
Section	**Officer**	**Time**	**Action**	**Initials**
Command	**Incident Commander**		Conduct regular briefings and situation updates with Command Staff and Section Chiefs to determine the situation status and timelines for restoration of services.	
			Continue to implement operational periods and update incident objectives within the Incident Action Plan.	
	Public Information Officer		Establish a central information center as needed to address all staff or patient care issues that may arise as a result of the disruption.	
			Update patients, staff, and visitors on situation status.	
			Address social media issues as warranted; use social media for messaging as situation dictates.	

	Liaison Officer		Continue to update local emergency management and other officials regarding situation and hospital status.	
	Safety Officer		Conduct ongoing analysis of existing response practices for health and safety issues related to patients, staff, and hospital; recommend corrective actions and update HICS 215A as required.	

Intermediate/Extended Response (2 to greater than 12 hours)				
Section	**Branch/Unit**	**Time**	**Action**	**Initials**
Operations	**Section Chief**		Prepare for demobilization and system recovery.	
			Recommend, in collaboration with Operations Section, when to resume normal activities and services.	
			Evaluate the need to shelter-in-place or evacuate patients to ensure safety.	
	Medical Care Branch Director		Continue patient care and management; identify patient care systems that are affected during the course of the restoration process.	
	Infrastructure Branch Director		Assess affected environmental systems and modify response actions as necessary.	
	Security Branch Director		Continue hospital security as well as traffic and crowd control.	
	Business Continuity Branch Director		Continue to implement the Business Continuity Plan and procedures.	
Planning	**Section Chief**		Ensure that updated information and intelligence is incorporated into the Incident Action Plan. Ensure the Demobilization Plan is being implemented.	
	Resources Unit Leader		Initiate staff and equipment tracking.	
	Situation Unit Leader		Update and revise the Incident Action Plan.	
			Initiate patient and bed tracking.	
	Documentation Unit Leader		Collect documentation of actions, decisions, and activities.	
	Demobilization Unit Leader		Prepare for demobilization and system recovery.	

Logistics	**Section Chief**		Recommend, in collaboration with Operations Section, when to resume normal activities and services.	
	Service Branch Director		Provide alternate documentation systems and support hardware (i.e., providing laptops and printers to affected areas for temporary use until systems are fully restored).	
			Monitor computer systems for new cyber threats.	
			Plan for migration of manual documentation to electronic processes after systems are restored.	
	Support Branch Director		Continue to obtain needed supplies, equipment, medications, food and water. Route requests for additional resources not available in the hospital through the Liaison Officer to outside agencies.	
Finance/ Administration	**Section Chief**		Refer to the Job Action Sheet for appropriate tasks.	
	Time Unit Leader		Consider alternate methods to ensure payroll processing and documentation of hours worked.	
			Track hours associated with the emergency response.	
	Cost Unit Leader		Monitor and track costs related to the disruption of information technology systems including the compromise of automated systems.	

Demobilization/System Recovery

Section	Officer	Time	Action	Initials
Command	**Incident Commander**		Declare incident termination.	
			Monitor full system recovery and the return to normal operations.	
	Public Information Officer		Issue a final media update with hospital status and appropriate service disruption information, in collaboration with the Incident Commander.	
	Liaison Officer		Communicate final hospital status and termination of the incident to the regional medical health coordinator, local Emergency Operations Center, area hospitals, local emergency medical services, and officials.	

	Safety Officer		Monitor the safe restoration of services and systems.	

Demobilization/System Recovery				
Section	**Branch/Unit**	**Time**	**Action**	**Initials**
Operations	**Section Chief**		Monitor the restoration of normal operations; coordinate with the Planning Section to ensure cancelled procedures and appointments are addressed.	
	Medical Care Branch Director		Restore patient care and management activities, including normal staffing plan.	
			Notify risk management and legal services of any actual or potential protected health information compromises or violations.	
	Security Branch Director		Re-establish security systems that may have been impacted by the incident.	
	Business Continuity Branch Director		Monitor and assist with restoration of information technology systems, utilities, and communications.	
Planning	**Section Chief**		Finalize and distribute the Demobilization Plan.	
			Conduct debriefings and hotwash with: ☐ Command Staff and section personnel ☐ Administrative personnel ☐ All staff ☐ All volunteers	
			Write an After Action Report and Corrective Action and Improvement Plan for submission to the Incident Commander, including: ☐ Summary of the incident ☐ Summary of actions taken ☐ Actions that went well ☐ Actions that could be improved ☐ Recommendations for future response actions	
	Documentation Unit Leader		Collect, organize, secure, and file incident documentation.	
			Prepare a summary of the status and location of all patients, staff, and equipment. After approval by the Incident Commander, distribute it to appropriate external agencies.	

	Demobilization Unit Leader		Monitor that the status of all impacted clinical and support operations are relayed to the appropriate sections for resolution.	
Logistics	**Section Chief**		Monitor the restoration of normal operations; coordinate with the Planning Section.	
			Inventory all Hospital Command Center and hospital supplies and replenish as necessary, appropriate, and available.	
	Service Branch Director		Prepare a summary report of corrective actions and recommendations for updating and improving diagnostic and protective cyber services.	
	Support Branch Director		Provide behavioral health support and information about community services to staff, as needed.	
Finance/ Administration	**Section Chief**		Compile a final summary of response and recovery costs and expenditures and estimated lost revenue. Submit to the Planning Section Chief for inclusion in the After Action Report.	
	Time Unit Leader		Ensure receipt of all personnel time sheets and documentation needed for the recovery of costs.	
	Compensation/ Claims Unit Leader		Contact insurance carriers to assist with initiating reimbursement and claims procedures.	

Documents and Tools

Emergency Operations Plan, including:

- ☐ Information Technology (IT) Failure Plan
- ☐ IT systems diagnostics (e.g., antivirus, spyware, firewall)
- ☐ IT systems malfunction alert notification process
- ☐ Business Continuity Plan
- ☐ Memoranda of Understanding with appropriate entities
- ☐ Paper charts and electronic medical record downtime procedures
- ☐ Patient, staff, and equipment tracking procedures
- ☐ Security Plan
- ☐ Utility Failure Plan
- ☐ Discharge Policy
- ☐ Hospital and campus maps, blueprints and floor plans
- ☐ Emergency Procurement Policy
- ☐ Risk Communication Plan
- ☐ Interoperable Communications Plan
- ☐ Demobilization Plan

Forms, including:

- ☐ HICS Incident Action Plan (IAP) Quick Start
- ☐ HICS 200 – Incident Action Plan (IAP) Cover Sheet
- ☐ HICS 201 – Incident Briefing
- ☐ HICS 202 – Incident Objectives
- ☐ HICS 203 – Organization Assignment List
- ☐ HICS 205A – Communications List
- ☐ HICS 214 – Activity Log
- ☐ HICS 215A – Incident Action Plan (IAP) Safety Analysis
- ☐ HICS 221 – Demobilization Check-Out
- ☐ HICS 251 – Facility System Status Report
- ☐ HICS 253 – Volunteer Registration
- ☐ HICS 254 – Disaster Victim/Patient Tracking
- ☐ HICS 255 – Master Patient Evacuation Tracking

Job Action Sheets

Paper forms for downtime documentation, data entry, etc.

Access to hospital organization chart

Television/radio/internet to monitor news

Telephone/cell phone/satellite phone/internet/amateur radio/2-way radio for communication

Position	Immediate	Intermediate	Extended	Recovery
Incident Commander	X	X	X	X
Public Information Officer	X	X	X	X
Liaison Officer	X	X	X	X
Safety Officer	X	X	X	X
Operations Section Chief	X	X	X	X
Medical Care Branch Director	X	X	X	X
Infrastructure Branch Director	X	X	X	X
Security Branch Director	X	X	X	X
Business Continuity Branch Director	X	X	X	X
Planning Section Chief	X	X	X	X
Resources Unit Leader		X	X	X
Situation Unit Leader	X	X	X	X
Documentation Unit Leader	X	X	X	X
Demobilization Unit Leader		X	X	X
Logistics Section Chief	X	X	X	X
Service Branch Director	X	X	X	X
Support Branch Director	X	X	X	X
Finance /Administration Section Chief		X	X	X
Time Unit Leader		X	X	X
Compensation/Claims Unit Leader				X
Cost Unit Leader		X	X	X