A. **Subject:** Incident Management Procedure

B. **Effective Date:** **April 15, 2019**

C. **Revised:** February 25, 2019

D. Procedure:

1. **Incident Process**
    a. **Primary Goal** - The primary goal of the Incident Management process is to restore normal service operation quickly and minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

    b. **Process Definition** - Incident Management includes any event which disrupts, or which could disrupt, a service. This includes events which are communicated directly by customers or calls made through the Help Desk.

    c. **Objectives** - Provide a consistent process to track incidents that ensures:
    - Incidents are properly registered
    - Incidents are properly assigned
    - Incident status is accurately reported
    - Queue of unresolved incidents is visible and reported
    - Incidents are properly prioritized and handled in the appropriate sequence
    - Resolution provided meets the requirements of the customer

    d. **Definitions**

        i. **Impact** – Impact is determined by how many personnel or functions are affected. The impact of an incident will be used in determining the priority for resolution. There are four grades of impact.

        - 1 – Extensive/Widespread – Issue critically affects the primary business service, major application, or mission critical system. The primary business services and systems are defined in the HIT Event Storm Process. Characteristics of such issues include:
            - Business service is not accessible or not functional
            - Production system crashes
            - Data integrity at risk
            - Production backup and recovery operations fail
        - 2 – Significant/Large – The business service, major application, or system is seriously affected or implementation stopped. No acceptable workaround is available.
        - 3 – Moderate/Limited – The business service, major application, or system is moderately impacted, no data has been lost, and the business

service, application, or system is still functioning. The issue may be temporarily circumvented using an available workaround.

- 4 – Minor/Localized – Non-critical issues, general questions, enhancement requests, or documentation issues...

i. **Incident** – An incident is an unplanned interruption to an existing IT service or reduction in the quality of an IT service. Failure of any item, software or hardware, used in the support of a system that has not yet affected service is also an incident.

A design flaw does not create an incident. If the product is working as designed, even though the design is not correct, the correction needs to take the form of a service request to modify the design. The service request may be expedited based upon the need, but it is still a modification, not a repair.

ii. **Priority** – Priority is determined by utilizing a combination of the incident's impact and urgency. The prioritization determination is defined in section 3 b.

iii. **Response** – Time elapsed between the time the incident is reported and the time the status is changed to "In Progress".

iv. **Resolution** – Service is restored to a point where the customer can perform their job. In some cases, this may only be a work around solution until the root cause of the incident is identified and corrected. Time to resolution is included in the Incident SLA defined in section 3 c, and is measured in business hours (after hours and weekends are excluded) from the time the incident is received until the time it is resolved,

v. **Service Level Agreement** – Often referred to as the SLA, the Service Level Agreement is the agreement between Health Information & Technology and the customer outlining services to be provided, and operational support levels.

vi. **Service Level Target** – Service Level Target is a commitment that is documented in a Service Level Agreement and is based on service level requirements. It is needed to ensure that the IT service continues to meet stated operational requirements.

vii. Service Request (to support reference in Paragraph I) Incident)

viii. **Urgency** – Urgency is determined by how much the user is restricted from performing their work. There are four grades of urgency:

- 1 – Critical – The resolution is immediately necessary to prevent business impact. Change approval is needed by the CAB or e-CAB. These events often dictate initiation of the HIT Event Storm Process. This document is located at O:\ Health Information and

Technology\Admin On Call Materials\Health Information & Technology Help Desk Comm Plan.docx.

- 2 – High – The resolution is needed as soon as possible because of potentially damaging service impact.
- 3 – Medium – The resolution will solve irritating problems or missing functionality. This change can be scheduled.
- 4 – Low – This resolution will lead to improvements, changes in workflow or configuration. This change can be scheduled.

The urgency of an incident will be used in determining the priority for resolution.

2. **Roles and Responsibilities:**

a. **Help Desks**

i. Ensure that all incidents received are recorded in ITSM Incident Management.
ii. Identify nature of incidents based upon reported symptoms and categorization rules supplied by support groups.
iii. Prioritize incidents based upon impact to the users and Service Level Agreement guidelines.
iv. Delegate responsibility by assigning incidents to the appropriate support group for resolution based upon the categorization rules.
v. Prepare reports showing statistics of incidents resolved/unresolved.
vi. Resolve common issues when possible using available resources.
vii. Initiate an HIT Event Storm when dictated by the impact and urgency of the incident. This document is located at O:\ Health Information and Technology\Admin On Call Materials\Health Information & Technology Help Desk Comm Plan.docx.

b. **Support Group**

i. Composed of technical and functional staff involved in supporting HIT services.
ii. Correct the issue or define a work around to the customer that will provide functionality that approximates normal service as closely as possible.
iii. If an incident reoccurs or is likely to reoccur, notify the appropriate support groups and management so that root cause analysis can be performed and a standard work around can be deployed.
iv. Perform post-resolution customer review to ensure that all work services are functioning properly and all incident documentation is complete. Prior to closing ticket?
v. Responsible for incident documentation and closure in ITSM. It is important that the action to resolve is clearly documented in the Resolution field and/or the Work Detail in each incident. In particular, document work done in detail if re-assigning to another group of individual, including ensuring categories are accurate at closure.

c. HIT Managers

i. Serve as an escalation point for breached Incidents and take action accordingly.
ii. Communicate with the HIT Help Desk when a significant issue arises with operations, or an issue arises causing a significant number of customer calls. This may be but is not limited to the HIT Event Storm process. Provide periodic status updates to the HIT Help Desk during an outage or significant issue.

d. **HIT Administrator on-call**
   i. For critical, widespread events as defined by the HIT Event Storm process, the HIT administrator on-call serves to ensure appropriate support for customers and HIT team members.
   ii. The HIT administrator on-call stays informed of major planned changes by attending the weekly HIT Change Advisor Board
   iii. Serves as approver for emergency change requests during an outage or at other times as needed.
   iv. Represents HIT to Medical Center operations and leadership during an HIT Event Storm.
   v. Serves as point person for crafting and approving communications to customers during an HIT Event Storm.

e. Customer/Requestor/Operational Owner
   i. Timely response to communication

3. **Incident Prioritization, Target Times, and Escalation**

In order to adequately determine if Service Level Agreements are met, it will be necessary to correctly categorize and prioritize incidents quickly.

a. **Categorization & Prioritization**
   i. Identify service impacted, and escalation timelines.
   ii. Establish the urgency and impact of the incident. All incidents are important to the user, but incidents that affect large groups of personnel or mission critical functions need to be addressed before those affecting 1 or 2 people.
      1. Does the incident cause a work stoppage for the user or do they have other means of performing their job? An example would be a broken link on a web page is an incident but if there is another navigation path to the desired page, the incident's urgency would be low because the user can still perform the needed function.
      2. The incident may create a work stoppage for only one person but the impact is far greater because it is a critical function. An example of this scenario would be the person processing payroll having an issue which prevents the payroll from processing. The impact affects many more personnel that just the user.
      3. Typically an incident which directly, negatively impacts patient care delivery, with no workaround, should be designated a high priority.

b. **Priority Determination** – The priority given to an incident that will determine how quickly it is scheduled for resolution will be set depending upon a combination of the incident urgency and impact.

Priority

	Urgency			
	1 - Critical Resolution is necessary immediately to prevent severe business impact	2 - High Resolution is needed ASAP because of potentially damaging service impact	3 – Medium Solve irritating problems or missing functionality	4 – Low Improvements, changes in workflow or configuration
Impact				
1 – Extensive Issue critically affects primary business service, major application or mission critical system	1 – Critical	1 Critical	2 – High	4 – Low
2 – Significant Business service, major application, or system is seriously affected; no workaround	1 - Critical	2 – High	3 – Medium	4 – Low
3 – Moderate Business service, major application, or systems is moderately impacted	1 - Critical	2 – High	3 – Medium	4 – Low
4 – Minor Non-critical issues, general questions, enhancement requests, documentation issues	2 – High	3 – Medium	3 – Medium	4 – Low

c. **SLA and Escalation Rules** – Incident support for existing services is provided 24 hours per day, 7 days per week, and 365 days per year. Following are the current targets for response and resolution for incidents based upon priority.

Priority	Target Type Response - target is met when ticket is "In Progress" Resolution - target is met when ticket is "Resolved"	Goal	Email and text/page Assignee	Email and text/page Support Group Supervisor	Email and text/page Support Group Manager	Notify Helpdesk	Use Business Hours?
Critical	Response	30 Minutes	50% 100% 150% 200%	100%	150%	100%	No
High	Response	30 Minutes	50% 100% 150% 200%	100%	150%	100%	No
Medium	Response	60 Minutes	50% 100% 150% 200%	100%		100%	Yes
Low	Response	24 Hours	50% 100% 150% 200%	100%			Yes
Critical	Resolution	2 Hours	50% 100% 150% 200%	50%	100%	100%	No
High	Resolution	3 Hours	50% 100%	50%	100%		No
Medium	Resolution	7 Days			100%		No
Low	Resolution	14 Days					No

Medium (PCS groups)	Resolution	8 Hours	75%				Yes

4. **Incident Management Process Flow**

Requesting Customer:

a. Incidents can be reported by the customer or technical staff through various means, i.e., phone, email, or the MyHIT automated tool.

Process:

a. **Incident Logging**
   i. All incidents must be fully logged and date/time stamped. All relevant information relating to the nature of the incident must be logged so that a full historical record is maintained.

b. **Incident Categorization**
   i. All incidents should relate to one of the published services listed in the Service Catalog.
   ii. Is this actually a service request incorrectly categorized as an incident? If so, update the case to reflect that it is a work order and follow the appropriate work order process.
   iii. Has the issue already been reported by others? More people reporting the same issue means the impact of the issue is broader than what might have been reported at first. The impact needs to be recorded based upon current knowledge of the issue. The HIT Help Desk and Help Desk supervisor communicate verbally and via Skype when an issue becomes duplicative. Such incidents may be linked in ITSM.

c. **Incident Prioritization**
   i. Before an incident priority can be set, the urgency and impact need to be assessed. Once the urgency and impact are set, the priority can be derived using the prescriptive table listed under 3b.
   ii. Is this a priority 1 major incident? If so, then a service is unavailable in part or whole, the appropriate HIT management should be alerted to make certain any resources necessary to the resolution will be immediately made available. Certain major incidents will cause initiation of the HIT Event Storm process. The determination of whether an event qualifies for this process is defined within the HIT Event Storm document. This document is located at O:\ Health Information and Technology\Admin On Call Materials\Health Information & Technology Help Desk Comm Plan.docx.

d. **Initial Diagnosis**
   i. If the incident has been routed to the Help Desk, the Help Desk analyst will carry out initial diagnosis, using diagnostic scripts and known error

information to try to discover the full symptoms of the incident and to determine exactly what has gone wrong. If possible, the Help Desk analyst will resolve the incident and close the incident if the resolution is successful.

ii. If the Help Desk analyst cannot resolve the issue, the case will then be assigned to the group that supports the service. The support analyst will then research the issue to determine cause and remediation options.

iii. After possible resolution has been determined, it will be implemented.

iv. The support analyst will verify with the customer that the resolution was satisfactory and the customer is able to perform their work.

v. If the customer is satisfied with the resolution, the support analyst will proceed to closure, otherwise continue investigation and resolve.

e. **Incident Closure**

i. The analyst responsible for resolving the incident should check with the customer to ensure the issue is fully resolved and that the customer agrees that the incident can be closed. The analyst should also check the following:

1. Closure categorization – Check and confirm that the initial incident categorization was correct or, where the categorization subsequently turned out to be incorrect, update the record.
2. Gather any outstanding details and ensure that the incident record is documented so that a full historic record with sufficient level of detail is complete.
3. Ongoing or Recurring Problem? – Determine whether it is likely that the incident could recur and decide whether any preventive action is necessary to avoid this. If so, initiate preventive action.
4. Formal Closure – Formally close the incident record.
5. User satisfaction survey – A survey will be sent to the customer; upon closure, assess how well the incident was handled and make any adjustments as necessary to the incident management process.

5. **Incident Escalation**

Priority	Time Limit Before Escalation	Escalated To
4 – Low	3 business days	Manager
3 - Medium	4 hours	Manager
	If on-call contact cannot be reached during non-business hours	Manager
	If neither on-call contact or their manager cannot be reached during non-business hours	Senior Management
	48 hours	Senior Management
2 – High	2 hours	Manager

	If on-call contact cannot be reached during non-business hours If neither on-call contact or their manager cannot be reached during non-business hours 24 hours	Manager Senior Management Senior Management
1 - Critical	Immediate If manager cannot be reached or HIT Event Storm is indicated	Manager Senior Management HIT Admin On-Call

Incident Escalation Process Flow

Examine all open incidents and determine actions based upon incident priority.

a. **Is this a priority 1 (critical) incident?**
   i. If it is a critical priority incident, immediately notify HIT management personnel via the CL HIT Leadership Outage Exchange list. HIT Admin On-Call should be contacted by phone. Initiate an HIT Event Storm as indicated. This document is located at O:\ Health Information and Technology\Admin On Call Materials\Health Information & Technology Help Desk Comm Plan.docx.
   ii. The HIT Help will monitor the status of the priority 1 incident providing informational updates to management at a minimum of every 4 hours.
   iii. Has the incident been resolved? If not, continue to monitor.
   iv. If the incident has been resolved, the HIT Help Desk notifies HIT management of the resolution.

b. **Is this a priority 2 (high) incident?**
   i. If it is a priority 2 incident, route the incident to the on-call analyst performing the resolution. Notification will be via text message and email.
   ii. Has the time limit to resolve the incident elapsed?
      1. If the time limit to resolve has elapsed, notify the manager of the support group via text and email.
      2. Continue to monitor the incident.
   iii. Has the incident been resolved?
      1. If the incident has been resolved, the incident assignee notifies the customer and all personnel previously contacted of the resolution.

c. **Is this a priority 3 (medium) incident?**
   i. If it is a priority 3 incident, route the incident to the on-call analyst performing the resolution. Notification is via text and email.
   ii. Has the time limit to resolve the incident elapsed?
      1. If the time limit to resolve has elapsed, notify the manager of the support group via text and email.
      2. Continue to monitor the incident.
   iii. Has the incident been resolved?
      1. If the incident has been resolved, the incident assignee notifies the customer and all personnel previously contacted of the resolution.