NCFHCC Patient Tracking & Monitoring Plan

PURPOSE & SCOPE

The 2015 North Central Florida Healthcare Coalition (NCFHCC) Patient Tracking Monitoring Plan outlines: 1) how patients are currently tracked by NCFHCC member organizations and 2) how the NCFHCC plans to help improve patient tracking in 2016 as a network. NCFHCC's service area is comprised of an 11-county region of Alachua, Bradford, Columbia, Dixie, Gilchrist, Hamilton, Lafayette, Levy, Putnam, Suwannee, and Union counties.

The scope of this process is to document the existing plans and procedures in place to track patients by NCFHCC service area counties and the hospitals that serve them. This plan is to help NCFHCC member organizations handle a public health event or other emergency, threat, or impact to the health and medical system in the NCFHCC service area.

OPERATIONS

County EMS Agencies

Each county EMS agency uses a day-to-day system (e.g., CAD system, Zoll ePCR, EMergencyPro) to track the routine transfer of patients as a result of EMS calls. Most of the coordination takes place within county dispatch and communications centers. During a larger event, especially those with multiple casualties, most of NCFHCC's 11 counties have Mass Casualty Incident (MCI) protocols and procedures in place. These protocols and procedures are used when the number of injured exceeds the capabilities of the first arriving unit as well as larger scale MCIs. The MCI policies designate a transportation officer with the duty to track and ensure transport of victims to appropriate medical facilities. Based on the extent and number of victims of an event, the Emergency Operations Center Health and Medical Branch (ESF 8) would most likely be activated and work directly with on-scene Incident Command, Medical Branch Director and the Transportation Officer on patient tracking.

Hospitals

Each hospital uses a day-to-day electronic tracking system for patients. In the event of a system failure, paper tracking (with specific number assignment) is used to track and monitor the patients. Communication and coordination (admissions, discharge, etc.) is done via phone or fax.

When a local state of emergency is declared, additional actions are taken. Most hospitals open their EOC (or similar facility) and begin to follow their established MCI protocols and procedures. Bed capacity is entered into EMSystem to allow for regional

and statewide situational awareness of bed counts and availability. The transfer of patients, if needed in an evacuation situation, most likely uses a paper form (HICS 260 Form) that captures all pertinent patient information. This form is handed off with the patient.

Region 3 and Statewide

Previously, for specific events, the Regional Domestic Task Force (RDSTF) Region 3 created a plan to assist with patient movement, when necessary. The most recent event and subsequent plan for patient movement and tracking was for the Republican National Convention, held in Tampa in the summer of 2012. This plan, which relies on the relies on the State Level ESF8, established a Region 3 Patient Movement Team. A Region 3 Patient Movement Team comprised of Northeast Regional Domestic Security Task Force, FDOH staff, emergency management (EM), fire rescue, law enforcement and health facility representatives was established and responsibilities included:

- ✓ Identifying potential receiving facilities
- ✓ Identifying potential transportation resources
- ✓ Establishing aerial port of debarkation (APOD)
- ✓ Maintaining awareness of patient movements
- ✓ Coordinating with APOD's and receiving facilities to assure they are prepared to receive patients
- ✓ Tracking patients from evacuation to final disposition
- ✓ Patient return/repatriation

Monitoring and coordinating resources to support care and movement of persons with medical and functional needs in impacted counties is one of State ESF8's eleven core missions as described in Florida's Comprehensive Emergency Management Plan. In order to fulfill this mission, State ESF8 must be prepared to support facility evacuation or decompression for noticed incidents or events (storm-related pre-landfall or post-impact) or no-notice incidents (e.g., tornados, mass casualty incidents), as outlined in the 2013 State of Florida Patient Movement Support Standard Operating Guideline from the Florida Department of Health. Statewide healthcare system monitoring will be conducted and assistance provided when requested by local jurisdictions. This may include coordination and resource support from external partners through the State Emergency Response Team (SERT) or the Emergency Management Assistance Compact (EMAC).

Upon receipt of a *local* request, the State ESF8 Patient Movement Branch will be activated. The Patient Movement Branch will be comprised of the Patient Coordination Group (medical specialists with hospital and medical diagnosis proficiency). Regional Patient Coordinators (RPCs) have been identified in each region to assist in coordinating patient placement. An RPC is familiar with the healthcare system within his or her region or county and serves as a local point of contact for the State.

Upon request from *State* ESF8, an RPC will coordinate the placement of patients in appropriate facilities based on capability and capacity and the patients' acuity and required medical treatment/interventions.

NCFHCC

In the NCFHCC service area, day-to-day patient tracking and monitoring occurs hundreds of times daily. In a larger event, the ESF8 provides the structure that helps support and coordinate health and medical resources.

However, there are limitations in the service area. For instance, resources are limited, particularly in the highly rural North Central Florida counties. Technological limitations exist with the current EMSystems; it's limited in its capacity to handle volumes of entries and the training on the system is critical. Transportation resources are limited in large scale events, and there are a limited number of private ambulance services in the region. More training will help the coordination of NCFHCC resources and tracking.

In the identification of the strengths and weaknesses of the patient tracking and monitoring system, the NCFHCC is documenting potential needs, training opportunities, and funding opportunities. It is increasing its collaborations with relevant partners such as the North Central Florida Trauma Agency, the Council on Regional EMS, Rural Health Partnership, and the Florida Rural Health Association. With these partners, NCFHCC is currently building an interdisciplinary task force to improve patient tracking and monitoring amongst NCFHCC member organizations.

Exploration of a Potential Data Sharing Tool to Access Relevant Patient Health Information During an Emergency or Disaster Situation

The below section describes the health information sharing tool currently available in Region 3 for accessing comprehensive and up-to-date patient health information. This tool is already used for Health Information Exchange by several medical facilities in the NCFHCC service area. This tool has relevance for patient tracking & monitoring purposes during emergency and disaster situations, especially in cases where a patient's health information is needed to treat or transport patients. In 2016, the NCFHCC-led task force will be exploring this system's capacity for emergency and disaster uses.

Health Information Exchange & Patient Tracking and Monitoring

The NCFHCC service area has a dedicated Health Information Exchange ("MyHealthStory"). In 2009, its development was spearheaded by North Central Florida stakeholders including area physicians, hospitals and other medical facilities, healthcare professional associations, universities and other learning institutions, regional economic development organizations, workforce development boards, local governments, and the VA. MyHealthStory is connected to the Florida Health Information Exchange (validation stage as of Dec 2015).

At its most foundational level, MyHealthStory is a personal health record for patients and an integrated longitudinal medical record with patient health data exchange tools for healthcare providers, first responders, and medical facilities. This health information exchange is unique because the health record system for patients is on the same platform as the one for healthcare and emergency care professionals. Also, for every transmission, a full audit trail is readily available for providers and patients. Vetted healthcare and emergency professionals within North Central Florida may become activated and have the ability to use MyHealthStory for patient tracking in emergency situations and to access comprehensive and up-to-date patient health information. This system has been operational in North Central Florida since 2011.

Access to Data & Secure Messaging

With the proper consents (which are electronic and stored on MyHealthStory), patients, their medical providers, their families, and first responders have access to the patients' health information whenever and wherever it's needed. The data can be accessed anywhere Internet is available. Messages can be sent to patients and their families or amongst medical and emergency care providers. MyHealthStory's technological platform is comprised of federally-certified electronic health record technologies (CEHRTs), and the platform is the same one used by the Department of Defense so that service-men and –women can access and communicate about their health data anywhere in the world. This technology even includes behavioral health data; it has been implemented by behavioral health centers since July 2011 and satisfies their HIPAA and CFR 42 concerns and needs.

Security

MyHealthStory[SM] is powered by McKesson's RelayHealth technology. RelayHealth protects the privacy and confidentiality of all information transmitted with its highly secure, built-in 128-bit, secure-socket layer encryption technology. RelayHealth uses industry accepted security standards for developing its security posture. The company approaches security as an ongoing process for increasing and ensuring compliance to these standards. The following standards heavily influence the approach to RelayHealth's information security:

- PCI-DSS 2.0 www.pcisecuritystandards.org/security_standards Given that we process credit card transactions, we are required to comply with the credit card industry PCI standard.
- HIPAA, HITECH & Meaningful Use www.healthit.gov Compliance with the healthcare security standard is an obvious requirement. McKesson's Internal Audit department assesses HITECH compliance on an annual basis.
- CA SB1386 modeled state privacy laws These regulations define appropriate steps to ensure the protection of end user sensitive data as well as disclosure processes required in case of breaches.
- DIACAP www.diacap.org RelayHealth's services are used by the Department of Defense. DIACAP compliance is therefore a strong driver for the company's security posture. Because RelayHealth's service is built around the concept of "single instance, multiple tenants", all of its commercial customers benefit from the stronger posture required by the Department of Defense.
- NIST/NSA NIAP CCEVS www.niap-ccevs.org/cc-scheme
- OWASP Top 10 List www.owasp.com
- CIS Security www.cisecurity.org
- SAS70 Datacenter Compliance
- ISO 27001 Standards www.iso.org/iso/catalogue_detail?csnumber=42103
- SANS Security Practices www.sans.org
- Microsoft Patterns and Practices msdn.microsoft.com/practices

The below excerpts from the 2013 RelayHealth Security White Paper describes the security standards with which MyHealthStory (through its RelayHealth technology) complies.

Physical Security

Production Facility: Production servers are located within a SSAE16 SOC-1 Type II Compliant IBX data center. The facilities use state-of- the-art security systems featuring 2-factor zone-based authentication, alarm monitoring/intrusion detection, video imaging, closed-circuit television (CCTV) and audio intercom subsystems.

Access Control: The Access Control subsystem controls physical access to the buildings and through the various doors within the facilities. The reading devices are biometric hand geometry readers, which permit system users to identify themselves to the system along with a predetermined pin number and obtain authorized access into each secure area.

Environment

Uninterruptible Power Supply: The data center runs on clean power conditioned by an Uninterruptible Power Supply (UPS) system. The UPS system provides protection from energy spikes and surges experienced by the public sector. Backup and redundant generators guarantee an alternate power source, providing indefinite hours of additional uptime in the event of a utility or system failure. The generators have a minimum of 48 hours of fuel with multiple fuel providers for extended operation during an outage.

Network Security

Redundant Firewalls: RelayHealth uses redundant best-of-breed firewalls at various layers in the RelayHealth architecture to protect the network from the outside world. Auditing is enabled on all firewalls and filter routers to track unauthorized access attempts and abnormal traffic patterns. Firewall firmware is kept up to date to maintain a strong perimeter.

VPN Gateway: Access to all McKesson resources is protected by best-of-breed firewalls and requires two-factor authentication with unique client certificates. Access to the production environment is restricted to certified release and operations personnel only. Access within the environment is further restricted on an as-needed, audited and automatically expiring time window.

System Monitoring

Vulnerability Scanning: Vulnerability scans are performed at least once a week to insure that servers are hardened to current patching levels. Servers that are patched will have an ad-hoc scan run to confirm the particular vulnerability that has been addressed. Vulnerability scans are performed in worse-case scenarios using authenticated local network scanners.

Intrusion Detection: Network based intrusion detection systems are active on production and corporate networks. They are configured to monitor traffic within the networks. This configuration minimizes the number of false-positive alerts given that perimeter firewalls prevent most TCP/IP packets from entering internal networks. If the IDS detect high risk traffic, IT administrators are instantly emailed/paged.

Redundancy

Network Redundancy: To establish the highest levels of network availability for partners and customers, RelayHealth utilizes redundant, high-speed bandwidth connections to the major internet backbones. Fully redundant best-of-breed switches provide resiliency and high performance.

Server Redundancy: All key servers are redundant using load-balanced server farms, active/active or active/passive clustering architectures.

Security Redundancy: All security devices have redundancy. All dedicated firewalls are active fail-over clustered. The management VPN- Firewalls are active failover clustered and can maintain management access in the event of a single VPN server failure. Requisite authentication servers are configured in a high availability cluster to remove single points of failure.

Relevant Endorsements

MyHealthStory and CommunityHealth IT (the Florida non-profit that is the steward of MyHealthStory) are endorsed by Enterprise Florida—the business development arm of the State of Florida. CommunityHealth IT's leadership is recognized as a trusted source of health information technology (HIT) and health information exchange guidance by the Office of the National Coordinator (ONC, which oversees the nation's HIT efforts). In 2013, CommunityHealth IT's leadership received the ONC Critical Access and Rural Hospital Champion Award from the head of the ONC and is an appointed member of the OneFlorida Clinical Research Consortium and Data Trust Program.

Plan Maintenance

This Patient Tracking and Monitoring Plan will be maintained and improved by the NCFHCC. The plan will be approved by the NCFHCC Executive Board and updated annually. The effectiveness and accuracy of the plan will be evaluated after exercises or incidents.