EXHIBIT 7

HCC After Action Report / Improvement Plan

Instructions: The AAR/IP must be completed in full. If more than one exercise was conducted, please complete an AAR/IP for each.

Name of Healthcare Coalition: North Central Florida Healthcare Coalition

Contract Number: COP43

Name of Exercise: US Department of Homeland Security Cyber Tabletop Exercise for the Healthcare Industry: Medical Surge and Cybersecurity Tabletop Exercise

Type of Exercise:

X Tabletop Exercise
☐ Full Scale Exercise
☐ Functional Exercise
☐ Actual Event

Was exercise coordinated by the Bureau of Preparedness & Response, Training and Exercise Program Unit ? ☐ Yes X No

Exercise/Incident Physical Location: Putnam County Emergency Operations Center

Lead Agency: North Central Florida Healthcare Coalition

Date of Incident/Exercise: May 26, 2016
Start Time: 5/26/2016
End Time: 5/26/2016

Duration of Exercise/Incident (days or hours): 1.5 hours

Exercise Planning Team Leadership

Point of Contact:

Exercise Director:
Name: Deborah Kobza
Title: President/CEO
Agency: The Global Institute for Cybersecurity + Research
Street Address: Astronaut Memorial Foundation Bldg., M6-306
City, State, Zip: Kennedy Space Center, FL 32899
Phone: 904.476.7858

EXHIBIT 7

HCC After Action Report / Improvement Plan

Email: Deborah.Kobza@giscr.org

Annual Training and Exercise Workshop:

Training & Exercise Workshop Conducted: Choose an item.

Reviewed and evaluated priorities based on needs, findings, and corrective actions of:

- X Exercises
- ☐ Real incidents
- ☐ Training
- ☐ Risk assessments
- ☐ Improvement plans from previous exercises
- ☐ Area(s) for improvement identified
- ☐ Identified associated target capabilities
- ☐ Other: Click here to enter text.

Planning Team *(name and organizational affiliation):*

NCFHCC

Participating Organizations:

Organization Name	Organization Type
Rural Health Partnership	Rural Health Network (Florida Statutes)
North Central Florida Trauma Agency	Trauma Agency (Florida Statutes)
Council of Regional EMS	EMS professional network
Department of Health Suwannee	Health Department
UFHealth Shands Gainesville	Health System
Lake Butler Hospital	Health System
Department of Health Putnam	Health Department
Florida Department of Health	State public health agency
Milla Pediatrics	Pediatric Rural Health Clinic
Professional Association of Health Care Office Management Gainesville	Professional Association
Board of County Commissioners	Local Government

EXHIBIT 7
HCC After Action Report / Improvement Plan

Scenario Type: Medical Surge and Cybersecurity

Scenario:
Summarize the scenario or situation initially presented to players, subsequent key events introduced into play, and the time in which these events occurred.

The purpose of this tabletop exercise (TTX) was to create an opportunity for stakeholders within the Healthcare and Public Health critical infrastructure sector in the State of Florida to enhance their understanding of key issues associated with a medical surge and focused cyber attack, including coordination and information sharing amongst private entities and government agencies in response to an attack.

Three exercises were facilitated focusing on Florida healthcare incident response and coordination with other internal and external entities to a potential medical surge and cyber attack. The intent of the exercises is to improve the overall response posture and collective decision-making processes (normal operations and medical surge).

For each exercise scenario, the following areas were explored and examined:

- Organizational and inter-organizational response and recovery
- Inter-organizational information sharing and collaboration mechanisms with the HPH sector during a cyber incident
- Improving the understanding of potential impacts and cascading effects cyber intrusions can have within the HPH sector
- Organizational response policies, plans and protocols – identifying potential gaps.

The exercises were a facilitated, scenario-driven discussion that allowed participants to interact in accordance with their respective responsibilities and expertise to coordinate their response to a significant cyber event. The scenarios are plausible and events occurred as they were presented.

Exercise Scenarios:

1. Vignette 1: Ebola Outbreak Medical Surge
    a. Vignette 1.1; Electronic Health Records/Electronic Medical Records (EHRs/EMRs)
    b. Vignette 1.2: Medical Device Malfunction

Each of the vignettes opened with a scenario that provided the general context for participants to identify and discuss major concerns and formulate responses to the situation described.

Using information provided in the scenarios including situational “injects”, participants responded to medical surge and cybersecurity issues related to the specific theme of the presented vignette. These discussions were guided by the exercise Facilitator who also managed the time allotted for each vignette.

Vignette 1.0: Ebola Outbreak – Medical Surge (30 minutes)

Opening Scenario:

At 7pm on Friday, a 23-yeard old male walked into the Emergency Dept. with a 3-day of fever (101.5), muscle pain, and severe body aches. Past medical history is unknown. Vital Symptoms: Temp (101.5), Headache, Muscle Pain, Abdominal Cramps

Discussion/Timeline:

Upon further investigation, it is learned that the patient’s illness started with light fever and aches, and that he recently arrived in Florida to attend college. His route from the Sierra Leone included flights to London, JFK, MCO (Orlando), and bus terminals to a Florida rural area.

What isolation procedures would be enacted?

What personal protective equipment measures are prepared for the staff?

Who needs to be contacted with this information?

What contact tracing questions would the patient be asked?

It's discovered through conversations with the patient's roommate that the patient's brother, in Sierra Leone died from Ebola.

The patient's roommate also is feeling very sick with severe stomach cramping, fever and has been rushed to the Emergency Dept. by fellow students

Other students have reported to the university medical office experiencing increasing symptoms from stomach cramping, fever and body aches.

The Florida Department of Health has been notified and contact tracking has begun.

The first patient has begun vomiting and fever remains elevated.

What additional considerations, screening measures and infection control and direction need to be taken.

The patient's roommate's initial epidemiological data has shown second generation infections.

The initial patient's condition continues to deteriorate.

The CDC has been consulted and has recommended transport for these two patients to occur within 24 hours.

How would you prepare patients for transport?

How will you manage disposal of patient waste?

How do you prepare for the additional patients?

How do you communicate with family members and the media?

Vignette I Injects:

Your IT Director has issued an immediate notification that an organization-wide malware ransomware attack has hit the hospital locking employees out of their computers

Your Emergency Management Director has issued an immediate notification that a cyber attack has hit the power grid impacting Florida and Alabama utilities and regions are beginning to experience blackouts. Your hospital will be losing power in 20 minutes.

Sub-Vignette 1.1: Corrupted Electronic Health Records / Electronic Medical Records (30 minutes)

Opening Scenario:

Your healthcare organization is a major trauma center that triages and treats patients. Patient care is captured, tracked and reviewed via a remotely accessible electronic health records/electronic medical records (EHR/EMR) system that provides real-time, point of care, patient-specific clinical data.

Several weeks ago the software on your EHR/EMR system was updated and despite some very minor initial problems, the system has been operating well. Today it is not.

Discussion/Timeline:

You are experiencing clinical support computers that are receiving data slowly, do not respond, or freeze. Patient care is increasingly delayed as physicians and clinicians authenticate and verify patient EHR/EMR information through labor intensive and time-consuming, downtime manual paper procedures. (e.g., patient questioning, contacting families).

Amidst the treatment of patients with corrupt EHRs/EMRs, the center becomes rapidly overwhelmed and as new patients arrive, only life-threatening emergencies are accepted for emergency department treatment. Trauma staff members are complaining that the EHR/EMR system has virtually ground to a halt and is unusable. Administrator priorities shift to reaffirming EHR/EMR data integrity

Sub-Vignette 1.1 Injects

In response to a high number of complaints of suspicious events and slow network speed, an investigation by the center's off-site IT services contractor discovers malware. The technicians determine that malicious code has infected multiple network-level servers, and possibly desktop and mobile work stations.

IT support concludes that the Web and main network servers are infected with a worm that has altered or erased an indeterminate quantity of data fields containing relevant patient health and treatment plan information.

Sub-Vignette 1.2: Medical Device Malfunction

Opening Scenario:

IT support concludes that the Web and main network servers are infected with a worm that has altered or erased an indeterminate quantity of data fields containing relevant patient health and treatment plan information.

Medical device activities that are outsourced include product design, prototyping, manufacturing, and supply chain management. Alongside these are challenges in regulatory compliance and certification that all components and products are authentic. The reliability and surety of devices are becoming an increasingly public issue. In the wake of several high-profile safety incidents, many manufacturers are taking additional steps to ensure that their products are both safe and effective. It has been reported that several devices with the ability to be reprogrammed remotely via wireless technology are used within your healthcare organization with suspect reliability.

Sub-Vignette 1.2: Inject:

A new generation of implantable cardioverter defibrillators (ICDs) manufactured by multiple companies with components made in the United States, Asia, and Europe are now used by many healthcare organizations, including your own. The new generation of ICDs is intended to offer improved reliability and safety over older models, and a "reasonable assurance of safety and effectiveness" is touted by the manufacturers.

Failure rates of the newer ICDs across all manufactures have been tracked as below traditional averages. The United States Food and Drug Administration (FDA) has identified firmware as the primary cause of device problems. To gain a competitive advantage, one manufacturer decides to update the firmware of its in-stock ICDs, and incentivizes physicians and suppliers to replace the non-updated implants with the safer, more reliable ICDs.

Several weeks after undergoing replacement of an implanted device, three very similar reports of "adverse events" – including one death – are reported by patients who received the updated ICD at your hospital.

Exercise Scenario – Conclusion and Hot Wash

For each of the Exercise Vignettes, the Conclusion and Hot Wash focused on:

- From exercise discussion, identified overall strengths and weaknesses, improvement options (recommendations)
- Participants completed feedback forms.

EXHIBIT 7
HCC After Action Report / Improvement Plan

Number of Participants: *Insert the total number of Provider participants of each of the following exercise participant categories:*
Players - 11
Controllers - 1
Evaluators - 1
Facilitators - 2
Observers - 1
Victim Role Players – This exercise represented a medical surge with cybersecurity exercise injects. Participants represented (role-played) and discussed response and recovery protocols, processes and procedures from a physical and cybersecurity perspective.

EXHIBIT 7

HCC After Action Report / Improvement Plan

When rating the performance of the exercise please rate according to the description provided below.	
Rating	**Description**
Performed without Challenges	Tasks associated with the activity were completed in a manner that achieved the objective(s) and did not negatively impact the performance of other activities. Performance of this activity did not contribute to additional health and/or safety risks for the public or for emergency workers and it was conducted in accordance with applicable plans, policies, procedures, regulations and/or laws.
Performed with Some Challenges, but Adequately	Tasks associated with the activity were completed in a manner that achieved the objective(s) and did not negatively impact the performance of other activities. Performance of this activity did not contribute to additional health and/or safety risks for the public or for emergency workers and it was conducted in accordance with applicable plans, policies, procedures, regulations and/or laws. However, opportunities to enhance effectiveness and/or efficiency were identified.
Performed with Major Challenges	Tasks associated with the activity were completed in a manner that achieved the objective(s), but some or all of the following were observed: demonstrated performance had a negative impact on the performance of other activities; contributed to additional health and/or safety risks for the public or for emergency workers; and/or, was not conducted in accordance with applicable plans, policies, procedures, regulations, and/or laws.
Not Performed	Tasks associated with the activity were not completed in a manner that achieved the objective(s).
N/A	The task was not performed because it was not part of the exercise scenario.
These ratings must be reflected in the Improvement Plan	

EXHIBIT 7

HCC After Action Report / Improvement Plan

I. Healthcare System Preparedness	Performed without challenges	Performed with some challenges	Performed with major challenges	Not Performed	N/A
1. The HCC functioned as a coordinated entity during the response.	X	☐	☐	☐	☐
2. Memoranda of Understanding or similar documents were used share resources during the exercise or event.	☐	☐	☐	☐	X
3. Healthcare responders had the necessary skills for the response.	X	☐	☐	☐	☐
4. Each hospital participated in the exercise or event.	X	☐	☐	☐	☐
5. At least one of the following members participated in the exercise or event:					
• Long Term Care Facility	☐	☐	☐	X	☐
• EMS Provider or Agency	X	☐	☐	☐	☐
• Community Health Center or Federally Qualified Health Center	☐	☐	☐	X	☐
• Local County Health Department	X	☐	☐	☐	☐
• A decision-making representative from each of the remaining HCC essential member partners.	X	☐	☐	☐	☐

If performed with challenges or not performed, briefly describe: the challenges that occurred, why they occurred and potential improvements. If this task was not exercised, explain why:
Start here:

The invited long-term care facilities did not attend, nor did any of the FQHCs. However, Rural Health Clinics and local government, two other groups of HCC essential member partners, were represented. NCFHCC will work even harder to recruit FQHCs and LTC representatives to the table tops next time.

Preparedness challenges identified and discussed:

For Ebola Medical Surge:

- Availability of Facilities (airborne isolation rooms – negative pressure)
- Availability of (location and number for required staff) appropriate chemical suits and respiratory equipment
- Staff Education – Training regarding contact tracing (patient travel history and geography)
- One participating hospital advised just last week someone called thinking they may have an Ebola patient – patient was placed in an airborne isolation room
- One participating hospital had an isolation box made out of PVC and plastic (gurney inside) in case hospital did not have isolation facilitations available.
- Procedures and communication (information sharing)to ensure that a hospital can take multiple patients.
- One participating hospital noted that is is difficult to get to an isolation area.
- Transport and change stations noted.
- Personal treating patients required to be in Tyvek suit and insulated with plastic barrier.
- Work needed on how medical surge or long-term patients would truly be handled. Need to plan and coordinate how many patients can be transported to the CDC in Atlanta.
- One hospital does not have air conditioning capability on the generator for loss of power in the location where the Ebola patients would be located
- Incident command activated hospital-wide to put runners in place.
- Beyond hospital (ordering food, meds) must be accessed)

- Messaging and communications need to be uniform
- Need capability to use state system to send out messages statewide
- Florida and Local Law Enforcement – May need to be looped in.

For cybersecurity sub-exercises and injects:

- One participating organization advised information about the back-up data center in Jacksonville for lock-out protection against a cyber attack.
- One participating hospital uses EPIC and can fail-over to their back-up location providing "read-only" access to patient EMRs/EHRs using the Citrix application for EPIC
- Many staff do not know how to use paper records anymore if electronic data access wasn't available. In many instances, paper form is not even available. Printed copies of patient records are not available.
- MyHealthStory Community Health Information Exchange (HIE) provides copies of patient health data (health summaries and demographics) that can be used on behalf of patient care in an emergency situation of this type (redundancy). Florida HIE may also have helpful data.
- The NCF Healthcare Coalition has a system where health-related information can be communicated. But unsure about communication of cyber issues.
- For one participating hospital, a mobile network can be set-up
- Disaster teams can be initiative – bringing in computers, networks and mobile stations
- Data network trailers (belong to AHCAs)
- Refer to the Health Department's list of mission critical functions which are reflected in COOP plans
- Need to define what is most important to get back up first? Email? Database?
- Need to determine if malware can cascade affecting other equipment or is it isolated on one network?
- Need to have plans to support if loss of power is lasting or escalating – Increased situational awareness
- EOC would be activated to assist in information sharing.
- Departments of Health locations have internal notification systems.
- If medical records attack, EKG machines are linked to EPIC medical records. Concern relayed that other systems could be affected.
- Some hospitals may have 1-2 computers available per nursing stations to back-up with a couple hours of data..
- Networks must be segregated. Production networks segmented.
- Assessment needs to be made on attack potential on phone communications.
- IV pumps to EKG equipment ultrasound ALL are Windows-based and vulnerable.
- MRI is still running on XP operating system, increasing vulnerability to cyber attacks.
- Robotics and surgery items are firewalled.

II. Healthcare System Recovery	**Performed without challenges**	**Performed with some challenges**	**Performed with major challenges**	**Not Performed**	**N/A**
6. The HCC took steps to communicate with local Emergency management regarding the importance of re-establishing essential services (including power, water, telephone, internet, dialysis, emergency medical care, pharmacy, etc.) during the exercise or event.	X	☐	☐	☐	☐
7. The HCC member organizations were able to successfully implement aspects of their Continuity of Operations Plan (COOP) during the exercise or event. Including:	X	☐	☐	☐	☐
• Billing for payment with healthcare insurers	X	☐	☐	☐	☐

• Use of electronic medical records	☐	☒	☐	☐	☐
• Maintaining daily operations including providing services to regularly scheduled patients not impacted by the exercise or event.	X	☐	☐	☐	☐
8. The HCC member organizations were able to successfully transition back to normal operating procedures at the end of the event or exercise.	X	☐	☐	☐	☐

If performed with challenges or not performed, briefly describe: the challenges that occurred, why they occurred and potential improvements. If this task was not exercised, explain why:
Start here:

The table top was performed by utilizing exercise injects as described in "Scenario Type." These injects occurred during exercise representation of normal operations in order to exercise actual events that can happen and how participants would respond. Improvements noted included improving internal and external information sharing, and for smaller healthcare organizations to address.

Exercise responses included the following action steps.

- Practice Drills (High)
- ID Potential Threats (High)
- Staff – Staff drops significantly for the night shift, but can recall staff (Medium)
- Contract local FLDOH to find/direct PT (Low)
- Understand Mission Critical Functions (High)
- Staff Training (High)
- Maintaining Situational Awareness to Support Recovery (High)

III. Emergency Operations Coordination	**Performed without challenges**	**Performed with some challenges**	**Performed with major challenges**	**Not Performed**	**N/A**
9. In-patient HCC member organizations were able to report their maximum patient bed capacity by type within four hours.	X	☐	☐	☐	☐
10. HCC member organizations that provide in-patient care were capable of surging 20% over the baseline established by the HCC.	X	☐	☐	☐	☐
11. If Patient Movement was tested, the HCC was able to communicate either need or available resources to local ESF8.	☐	☒	☐	☐	☐

If performed with challenges or not performed, briefly describe: the challenges that occurred, why they occurred and potential improvements. If this task was not exercised, explain why:
Start here:

Exercise responses included the below action steps (Priorities – High, Medium, Low). The group agreed that we need to better coordinate communications of need and available resources.

- Use EOC as Center of Communication for EPI/Cyber (High)
- Review PIO Trainings (depth/multiple (Low)
- Training related to planning for cyber threats (Medium)

- While many mass casualty plans/medical surge plans exist, coalition can "bridge the gap" by assisting in planning role to this subject (Medium)
- Identify and conduct appropriate vendors for IR (Medium)
- Continue to improve information security awareness (HIGH)
- Help develop IT cyber intrusion protocols (Medium)
- Train staff
- Meeting to develop medical surge and transport procedures for infectious diseases (High)
- Develop and implement cybersecurity and resilience policies (High)
- Communication and messaging policies for cyber threats (Medium)
- Increase time for table-top exercises (Medium)

IV. Fatality Management	**Performed without challenges**	**Performed with some challenges**	**Performed with major challenges**	**Not Performed**	**N/A**
13. HCC member organizations were able to implement individual Fatality Management plans.	☐	☐	☐	☐	X
14. HCC member organizations were able to coordinate short-term management of fatalities that overwhelm local morgue capacity.	☐	☐	☐	☐	X
15. The HCC was able to communicate the availability of morgue resources to local ESF8.	☐	☐	☐	☐	X

If performed with challenges or not performed, briefly describe: the challenges that occurred, why they occurred and potential improvements. If this task was not exercised, explain why:
Start here: Mass fatalities were not a part of this table top. The initiation of a medical surge was the concentration.

V. Information Sharing	**Performed without challenges**	**Performed with some challenges**	**Performed with major challenges**	**Not Performed**	**N/A**
16. HCC member organizations were able to communicate the following Essential Elements of Information (EEIs) to the HCC within the established time frames:					
• Facility operating status	X	☐	☐	☐	☐
• Facility structural integrity	X	☐	☐	☐	☐
• Evacuation plans vs. shelter-in-place	X	☐	☐	☐	☐
• Available resources (including staff, supplies, medications, equipment, etc.)	X	☐	☐	☐	☐
• Any immediate needs of the member organization	X				
17. HCC member organizations communicated using interoperable communications systems.	X	☐	☐	☐	☐
18. The HCC communicated HCC member organization EEI's to local ESF8 and the local county health department.	X	☐	☐	☐	☐
19. The HCC communicated the following to HCC member organizations, if applicable					
• Location of Family Assistance Centers (to include patient transfer locations and	☐	☐	☐	☐	☒

fatality management) • Status of essential healthcare services • Status of critical services, such as electric, water, sanitation, heating, etc. • Social distancing advisories • Boil water advisories • Vaccine administration protocols and points of distribution	☐ ☒ ☐ ☐ ☐ ☐	☐ ☒ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐ ☐	☐ ☐ ☒ ☒ ☒

If performed with challenges or not performed, briefly describe: the challenges that occurred, why they occurred and potential improvements. If this task was not exercised, explain why:
Start here:

Information sharing communications were addressed regarding communications with internal and external organizations to respond to the medical surge and the cybersecurity exercise injects included a central hospital facility being:

- Attacked by ransomware resulting in employees being locked out of computers
- Electronic health records/electronic medical records computer functionality degradation from malicious code that infected multiple network-level sensors, desktop, and mobile workstations
- Loss of data containing relevant patient health and treatment plan information
- Medical Device malfunction and failures – Communication/information sharing with local/state/FDA, patients and the media – responding to adverse events including one death who had received the medical device at the hospital
- Depending upon communications and information sharing with internal and external resources to compensate for loss of computer functionality and data loss (communications with off-site back-up computer centers, staff

Critical services such as electric, water, sanitation, and heating was addressed; however, there were issues identified such as having to keep Ebola patients in place at Shands if the power went out and having to move in A/C units to keep those patients comfortable because the generators are not hooked up to the A/C system in the North Tower (where the isolation beds are).

VI. Medical Surge	**Performed without challenges**	**Performed with some challenges**	**Performed with major challenges**	**Not Performed**	**N/A**
20. HCC member hospitals implemented Crisis Standards of Care per their Emergency Operations Plan.	X	☐	☐	☐	☐
21. HCC member hospitals and other in-patient member facilities decompressed to achieve bed availability 20% above the HCC-established baseline.	X	☐	☐	☐	☐
22. The process for HCC member organizations to request and receive resources (such as equipment, supplies, pharmaceutical caches, and staff) was successfully executed.	☐	X	☐	☐	☐

If performed with challenges or not performed, briefly describe: the challenges that occurred, why they occurred and potential improvements. If this task was not exercised, explain why:
Start here:

Organizations other than perhaps Shands, particularly rural ones, have a hard time understanding which PPEs they need. They also don't have the epidemiology resources they need in place and will be leaning heavily on Alachua Department of Health. The other organizations planned to use first responders to address Ebola medical surge situations; however, testing and training of proper PPE and PPE use is costly and time-intensive. It's something that the NCFHCC needs to help the service area address.

EXHIBIT 7

HCC After Action Report / Improvement Plan

Exercise responses included the following action steps. (Priorities – High, Medium, Low)

- Meeting to develop medical surge and transport procedures for infectious diseases (High)

VII. Responder Safety and Health	Performed without challenges	Performed with some challenges	Performed with major challenges	Not Performed	N/A
23. HCC member organizations had adequate and proper function Personal Protective Equipment to respond to the exercise or event.	☐	☐	X	☐	☐
24. HCC Behavioral/Mental Health member organizations were able to provide emergency and psychological medical care when needed.	☐	☐	☐	☐	X
25. The HCC had access to adequate post-exposure prophylaxis.	☐	X	☐	☐	☐

If performed with challenges or not performed, briefly describe: the challenges that occurred, why they occurred and potential improvements. If this task was not exercised, explain why:
Start here:

Organizations need to work in the area of understanding what PPE is appropriate for their responsibilities.

VIII. Volunteer Management	Performed without challenges	Performed with some challenges	Performed with major challenges	Not Performed	N/A
26. The HCC performed the following:					
• Identify and roster volunteers	☐	☐	☐	☐	X
• Receive volunteers	☐	☐	☐	☐	X
• Determine volunteer affiliation	☐	☐	☐	☐	X
• Confirm volunteer credentials	☐	☐	☐	☐	X
• Assign roles and responsibilities to volunteers	☐	☐	☐	☐	X
• Provide just-in-time training to volunteers	☐	☐	☐	☐	X
• Track volunteers	☐	☐	☐	☐	X
• Out-process volunteers	☐	☐	☐	☐	X

If performed with challenges or not performed, briefly describe: the challenges that occurred, why they occurred and potential improvements. If this task was not exercised, explain why:
Start here: Volunteers were not discussed for the Ebola medical surge or cybersecurity threat scenarios. Volunteers have not yet been addressed because specialized first responders are initially to be used for this highly contagious condition.

Exercise Events Summary & Conclusion

INSTRUCTIONS: This section must summarize what actually happened during the exercise in a timeline format (i.e., the actions that were actually presented to the players and the actions the players took during the exercise).

EXHIBIT 7

HCC After Action Report / Improvement Plan

Provide a conclusion describing the overall exercise as successful or unsuccessful, and briefly state the areas in which subsequent exercises should focus.

Start here: The purpose of this tabletop exercise (TTX) was to create an opportunity for stakeholders within the Healthcare and Public Health critical infrastructure sector in the State of Florida to enhance their understanding of key issues associated with a medical surge and focused cyber attack, including coordination and information sharing amongst private entities and government agencies in response to an attack.

EXHIBIT 7

HCC After Action Report / Improvement Plan

Exercise Events Summary:

Over a 90-minute period, three exercises were facilitated focusing on Florida healthcare incident response and coordination with other internal and external entities to a potential medical surge (Ebola) and cybersecurity attacks and loss of functionality . The intent of the exercises is to improve the overall response posture and collective decision-making processes (normal operations and medical surge).

For each exercise scenario, the following areas were explored and examined:

- Organizational and inter-organizational response and recovery
- Inter-organizational information sharing and collaboration mechanisms with the HPH sector during a cyber incident
- Improving the understanding of potential impacts and cascading effects cyber intrusions can have within the HPH sector
- Organizational response policies, plans and protocols – identifying potential gaps.

The exercises were a facilitated, scenario-driven discussion that allowed participants to interact in accordance with their respective responsibilities and expertise to coordinate their response to a significant cyber event. The scenarios are plausible and events occurred as they were presented.

Exercise Scenarios:

Vignette 1: Ebola Outbreak Medical Surge

Vignette 1.1; Electronic Health Records/Electronic Medical Records (EHRs/EMRs)

Vignette 1.2: Medical Device Malfunction

Exercise Events and Timeline:

Time allotted for this exercise: 90 minutes.

Each of the vignettes opened with a scenario presented by the Facilitator that provided the general context for participants to identify and discuss major concerns and formulate responses to the situation described.

Participants were divided into two groups, each group discussing the scenarios and injects as they occurred, and how each organization and individual participating in the exercise would respond.

Using information provided in the scenarios including situational “injects”, participants responded to medical surge and cybersecurity issues related to the specific theme of the presented vignette. These discussions were guided by the exercise Facilitator who also managed the time allotted for each vignette.

Conclusion:

At the conclusion of the individual group discussions for each of the exercise vignettes, each group then presented to the group as whole for further discussion of current state and opportunities for improvement.

The overall exercise was successful having brought forth discussion around current state response and recovery and opened up areas, previously not addressed with regard to cybersecurity – areas needing to be addressed and improved. Exercise results from participants indicated a good realistic scenario and that more exercise time was needed and desired.

Participant Exercise Rating:

The exercise was well structured and organized: (4.6)
The exercise scenario was plausible and realistic: (4.7)
The multimedia presentation helped the participants understand and become engaged in the scenario: (4.7)
The facilitator(s) was knowledgeable about the material, kept the exercise on target, and was sensitive to group dynamics: (4.8)
The Situation Manual used during the exercise was a valuable tool throughout the exercise: (4.1)

Participation in the exercise was appropriate for someone in my position: (4.4)
The participants included the right people in terms of level and mix of disciplines: (4.3)

EXHIBIT 7

HCC After Action Report / Improvement Plan

Major Strengths

INSTRUCTIONS: Please provide at least 3 major strengths of the exercise using the SMART format (specific, measurable, achievable, realistic, and time-framed).

Start here:

Medical Surge Triage

Situational Awareness and Coordinated Response Information Sharing

Response Plans / Business Continuity

Primary Areas for Improvement (Must be included in Improvement Plan)

INSTRUCTIONS: Please provide at least 3 primary areas for healthcare coalition improvement using the SMART format (specific, measurable, achievable, realistic, and time framed).

Start here:

Each of the areas of improvement defined below are specific, measurable, realistic and have a time-frame that will be needed for improvement.

Improve Response Communications (By June 2017)

- Improve communication among providers and emergency management regarding responsibilities
- Development regional response plan for cyber threat
- Many existing response plans can provide a framework for response to medical surge and cybersecurity
- Interdependent communication
- Outside contracts and contacts with Incident Response providers

Perform Additional Cybersecurity Trainings (By June 2017)

- Cybersecurity is not something we have done before. Good to have a new topic to discuss. Not enough time to go through each scenario – needed more time for the exercise.
- Possible need for a regional emergency information tech trailer
- Plans for cyber attacks
- Cybersecurity plan development
- Improve staff knowledge of IT vulnerabilities
- Improve - Equipment manufacturer information security
- Improve Vendor Cybersecurity Assurance
- Improve Medical Device Cybersecurity
- Improve FDA Medical Device Manufacturer Cybersecurity - Compliance

Business Continuity (By June 2017)

- How to revert to using paper backup to loss of IT system (This particular one is important for health systems that are using electronic records.)

EXHIBIT 7

HCC After Action Report / Improvement Plan

Additional action steps that should be taken to address the issues identified above. For each action step, indicate if it is a high, medium, or low priority.

Responses included:

- Practice drills **HIGH**
- ID Potential Threats **HIGH**
- Our staff drops significantly for night shift. But can recall staff **MEDIUM**
- Should be simple enough to contract our local FLDOH to find/direct PT **LOW**
- Use EOC as center of communication for EPI/Cyber **HIGH**
- Understand Mission Critical Functions **HIGH**
- Review PIO trainings (depth/multiple) **LOW**
- Training related to planning for cyber threats **MEDIUM**
- While many mass casualty plans/medical surge plans exist, coalition can "bridge the gap" by assisting in a planning role to this subject **MEDIUM**
- Identify and conduct appropriate vendors for IR **MEDIUM**
- FDA needs to encourage vendors to improve security **HIGH**
- Continue to improve information security awareness **HIGH**
- Provide PPT info and exercise to partners for them to use within their own organization **MEDIUM**
- Get with the correct people **HIGH**
- Help develop IT cyber intrusion protocols **MEDIUM**
- Train staff **LOW**
- Meeting to develop medical surge + transport procedures for infectious diseases **HIGH**
- Cybersecurity + resilience policies (other than SHANDS none are in place) **HIGH**
- Communication + messaging policies for cyber threats **MEDIUM**
- Have 5-10 more minutes for tabletop **MEDIUM**

Corrective actions that relate to areas of responsibility. Who should be assigned responsibility for corrective actions?

Responses included:

- Emergency Management @ UF Health
- ALL STAFF! Especially triage and clerks
- Utilization of our notification and recall list to have appropriate staff
- HIC report findings to DOH representative
- MCF (review each year but make it scenario-based)—Planner/SLT
- Develop communications plans and scripts for scenarios—PIO/Planner
- Review infections disease transport protocol
- Development of cyber response plan— NCFHCC with assistance of Global Forum
- Cyber preparedness training—NCFHCC
- Medical surge planning—NCFHCC
- IT—NCFHCC
- Planning/Training—NCFHCC
- Medical surge + transportation policies for infectious disease—NCFHCC
- Cyber resilience readings—CommunityHealth IT/ Global Forum
- Communication + messaging—NCFHCC

EXHIBIT 7
HCC After Action Report / Improvement Plan

Policies, plans, and procedures that should be reviewed, revised, or developed. Indicate the priority level for each.

Responses included:

- Triage/screening procedures with staff **MEDIUM**
- Staffing- will always be an ongoing issue **MEDIUM**
- Communication with DOH. Ensure correct contact information is up to date **MEDIUM**
- COOP **HIGH**
- Use of tabletops/presentations to prepare team **HIGH**
- NCFHCC All-Hazards Plan **LOW**
- NCFHCC COOP or development of MEF **MEDIUM**
- NCFHCC medical surge plan **HIGH**
- Review of IR procedures and policy **MEDIUM**
- Continue risk assessment process **HIGH**
- Plans for cyber attacks
- Develop IT cybersecurity plan
- Cyber resilience roadmap **HIGH**
- COOP for NCFHCC-add cyber **HIGH**
- FLDOH transport for Ebola **HIGH**

EXHIBIT 7

HCC After Action Report / Improvement Plan

After Action Report (AAR) Improvement Plan Matrix

Capability	Corrective Action Title	Recommendation	Corrective Action Description	Primary Responsible Agency	Agency POC	Start Date	Completion Date
1: Information Sharing	1. Information Sharing Plan (Addition to Communication Plan)	1. NCFHCC will lead region in information sharing trainings and meetings.	Results of those meetings will be put into a Information Sharing Plan and will become part of the Communications Plan	NCFHCC	Kendra Siler-Marsiglio	Aug 2016	Jun 2017
2. Medical Surge	2. Coordinate Patient Transport Plan with Medical Surge Planning	2. Ensure that the disaster and emergency preparedness stakeholders are informed about FLDOH patient transport protocols.	NCFHCC will ensure that the disaster and emergency preparedness stakeholders are informed about FLDOH patient transport protocols.	NCFHCC	Tony McLaurin	Aug 2016	Jun 2017
3. Volunteer Management	3. Define areas where volunteers can be used for medical surge caused by a highly infectious disease	3. NCFHCC can hold meetings to discuss the appropriate uses of volunteers for highly infectious disease disasters.	If areas are identified for volunteers, then NCFHCC will inform the region about these appropriate uses.	NCFHCC	Tony McLaurin	Aug 2016	Jun 2017
4. Choose an item.	3. Observation from Primary Areas for Improvement	4. Insert Recommendation	Insert Corrective Action	Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
5. Choose an item.	3. Observation from Primary Areas for Improvement	5. Insert Recommendation	Insert Corrective Action	Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.