IHA Clinical Services Emergency Preparedness

Innovative Learning and Training for Leading Healthcare Issues

IHA Illinois Health and Hospital Association

September 27, 2017

Hello Clinical Services members:

On November 15 from 9 a.m. to 12 p.m., IHA will conduct its annual Clinical Services Emergency Preparedness Exercise, a full-scale, state-wide simulation. This year's exercise involves a widespread cyberattack impacting multiple critical systems within healthcare organizations. Affected systems will range from biomedical devices to electronic medical records, with the option for facility-specific customization. Facilities will be tasked with response and recovery efforts, including developing and conducting recovery planning and maintaining mission essential functions. The exercise will use multimedia platforms to provide relevant scenario and exercise injects.

This year's scenario reflects feedback indicating that cyberattacks are among members' greatest organizational vulnerabilities and concerns. Recent international incidents demonstrate the very real danger cyber threats pose to healthcare institutions.

In February 2016, Hollywood Presbyterian Medical Center was struck by ransomware that crippled the institution. The hospital's computer network was held for a ransom of $17,000 in digital currency. While patient care was not impacted, communication devices such as hospital computers were unable to communicate with one another due to data re-encryption from an outside source. Normal operations were unable to resume until after the funds were paid and the hackers provided the encryption key.

In one of the more publicized ransomware attacks, earlier this year, hackers from a group known as Shadow Brokers attacked British healthcare infrastructure, as well as organizations and industries all over the world, with the Wannacry virus. Forty-eight medical facilities in the United Kingdom alone were affected by this cyber weapon, which was reengineered from U.S. National Security Agency hacking tools. The virus spread quickly, and within six hours, a vast number of computers within the British national health system had been infected. Patient care was impacted and caused diversion of critical patients to unaffected facilities. Numerous impacted organizations are still recovering and strengthening their digital infrastructure to mitigate future attacks.

Members are encouraged to register for the Clinical Services program to gain insight into addressing a multi-assault incident. The exercise will cover various operational components, including medical surge, command and control, resource management, security, continuity of operations, and communications. **The exercise can be modified and scaled to meet the specific needs of each participating facility.**

Objectives include:

- ✓ Evaluate current system and individual facility plans pertaining to cyberattacks, malware, ransomware, and other corruptions of electronic medical data critical to hospital operations.
- ✓ Qualitatively and quantitatively evaluate the effectiveness, sustainability and viability of system and facility downtime procedures.
- ✓ Identify mechanisms to manage the potential loss of protected health information as well as personally identifiable information.
- ✓ Identify non-corruptible information sharing methods for both intra-hospital and intra-regional communications.
- ✓ Evaluate regional and institutional strategies for managing media and stakeholder relations.
- ✓ Quantitatively and qualitatively evaluate recovery strategies and the procedures for prioritizing the return of services and infrastructure.
- ✓ Evaluate how facilities and systems can implement resource and staffing procedures in order to care for an influx of patients following an external event.

Participating hospitals and health systems will receive a pre-exercise video that will walk through a tabletop discussion of key actions prior to the full-scale exercise. Please share this message with appropriate staff and ask that they participate in this valuable learning opportunity. IHA suggests including staff from the following areas:

- ✓ Clinical Engineering
- ✓ Clinical Nursing
- ✓ Emergency Preparedness
- ✓ Facilities
- ✓ Information Technology
- ✓ Media Relations
- ✓ Risk Management
- ✓ Purchasing
- ✓ Other members of the Incident Command Team

Click Here to Register

After registering, participants will receive a confirmation email with information about joining the exercise. Please contact Keneatha Johnson at **kjohnson@team-iha.org** with any questions.