Emergency Preparedness Symposia & HIT Security Planning

A more meaningful and useful Emergency Preparedness Symposium (EPS)

DOHMH met with representative EPCs in April 2015 to review the EPS. EPCs noted outcomes they wanted:

> ***For consistency, all meetings should have the same format. It is valuable for experts to present on and to structure work sessions to help EPCs complete deliverables. Structured networking during an extended break with presentations and posters of innovations produced by fellow EPCs is valuable. Each meeting should focus on a topic that the GNYHA, NYC EM and DOHMH are working on.***

The EPSs this year are intended to yield these outcomes. Additionally, EPCs expressed a desire to exercise with DOHMH. Addressing this, DOHMH will work in parallel with our EPS planning team as the agency plans and conducts a cyberattack exercise (December, 2015). We will use the EPS and its breakout sessions as a forum to ensure hospitals progress on healthcare information technology (HIT) security and cyberattack planning and then hold a final EPS in which DOHMH will facilitate a discussion with the group on cyberattack.

Why HIT Security and Cyberattack?

Cyberattacks have happened in our own back yard (Kingsbrook Hospital) and worldwide at Sony, and are occurring with greater frequency. DOHMH has prioritized a cyberattack exercise to bolster the agency's response.

What do we mean by HIT security and cyberattack? A working definition.

PROTECTION against the attack: Use basic knowledge of how attacks take place and actions that increase system vulnerability (e.g., what do clinician/nurse/lab tech etc. use in daily patient care that is at risk of attack and are there behaviors staff can adopt to decrease risk? Facility level protection is essential to protection at the system level.

SURVEILLANCE/IDENTIFICATION of a cyberattack: What hospital IT systems are in place for this? What should hospital staff look for? What is the protocol for hospital staff to report suspected cyberattacks, patient data or equipment (e.g., pharmacy robot) errors? How do we increase awareness of HIT security threats among staff?

RESPONSE during an attack: Once identified, who is part of the "response team" and what are their goals? How do they communicate with clinicians and patient care staff? How do they end the attack? How does the facility continue to care for patients during extended disruption of HIT?

How will planning take place for the EPS and the cyberattack discussion?

A volunteer group of hospital EPCs will serve as a core team to plan the EPS. They will attend DOHMH's cyberattack exercise planning meetings and bring expertise from this experience and their own hospital HIT staff to the EPS planning. They will help conduct extended breakout sessions at the EPS, allowing all hospitals to outline their cyberattack strategies. To facilitate this, BP4's EPS will be 4 hours in length.

What should I expect?

The EPS will be similar to past years with guest speakers and structured networking. We will dedicate the final 2 hours of the EPS for breakout groups for HIT security planning. The first 2 EPS will focus on HIT security and/or communications. For the last EPS, hospitals will participate in a facilitated discussion with a cyberattack scenario.

As the EPC, what will my roles and obligations be?

Attend 3 EPS. During breakouts, contribute to discussion leading to developing your own facility's cyberattack risk assessments, strategies or plans. Between EPSs, implement cyberattack planning activities at your facility. Participate in a facilitated discussion DOHMH will facilitate. After the third EPS, submit documentation (TBD) showing cyberattack planning activities for your facility. List any actions DOHMH should take for citywide cyberattack planning or any actions where DOHMH needs to interact with other healthcare preparedness partners to promote HIT security preparedness system wide. Send this to Darrin Pruitt at dohmhcore@health.nyc.gov.