HIPAA and the Emergency Preparedness Plan

As you work through your Emergency Preparedness Plan for your RHC or FQHC, keep in mind that you may already have some of the requirements in place through your HIPAA compliance program. Some of the requirements of the Emergency Preparedness Plan overlap with HIPAA so you won't have to "reinvent the wheel" as they say. Let's look at a few of those areas in your HIPAA security program where they both intersect.

Emergency Plan Risk Assessment: You are required to conduct a risk assessment utilizing an all-hazards approach and it must be facility based or you can rely on a community-based risk assessment. The risk assessment requires you to look at all probable emergencies. You will look at natural emergencies that can occur in your area and develop strategies for responding to those emergencies. Under the HIPAA security rule, you are also required to conduct a risk analysis to look at threats and vulnerabilities to your electronic systems that hold e-PHI, and threats to your facility that holds the electronic systems. So, you may already have a plan for natural hazards such as tornadoes or flooding, and other acts of God. Your HIPAA disaster recovery plan which is part of your HIPAA contingency plan, should have guidance for responding to loss of data due to network outage or power outage and how to recover the lost data. Your HIPAA disaster recovery plan will tell you how to respond to an emergency and how to operate in emergency mode. So, look at your HIPAA risk analysis and your HIPAA Contingency Plan for commonality with the Emergency Plan Risk Assessment.

Communication Plan: You are required to develop a communication plan with contact names and numbers for staff, any entities providing you services under an agreement, patient's physicians, other RHCs/FQHCs, volunteers, Federal, State, or local emergency preparedness staff and other sources of assistance. Is there a HIPAA parallel? While HIPAA does not directly ask you to establish a communication plan, all organizations develop some sort of plan to contact key personnel in the event of an emergency that threatens
e-PHI. Sometimes it is called a recall plan and often found in your disaster recovery plan and emergency operations mode plan. So, look at this part of your HIPAA program for a contact list that already exists and build from it to meet the requirements of the Emergency Preparedness Plan.

Training and Testing: You are required to provide emergency preparedness training and conduct testing of your plan. You must provide initial emergency preparedness training to new staff members and at least annually thereafter. The training must be provided to every staff member and should explain their role during an emergency. This also includes any volunteers you have on staff. The training must reflect the risks identified in the facility's risk assessment.

As for testing, you are required to participate in a full-scale community based exercise, but if not available, a facility exercise is appropriate. All staff members must participate in the exercise. You are required to conduct two exercises annually and the second one may be a table top exercise. This testing is designed to address any training gaps that require correction. Again, you may have already participated in an exercise under your HIPAA security program. The security rule, under the administrative safeguards and the contingency plan standard, includes an implementation specification called "testing and revision procedures". Under this standard, you are required to periodically test your contingency plan. Therefore, look to your periodic testing of your contingency plans for overlap with the emergency preparedness plan. If you had a real-world event requiring you to initiate your emergency response, you may use it to meet one of your two exercise requirements under the emergency preparedness plan.

Policies and Procedures: You are required to develop and implement emergency preparedness policies and procedures. In addition to including documentation for the overall plan itself, the risk assessment, your communication plan, your training and testing procedures and outcomes, you must also include policies and procedures for the following:

Continued on pg. 2…

HIPAA & the Emergency Preparedness Plan…

- Safe evacuation from the RCH/FQHC
- Shelter in place plan
- Medical records preservation procedures
- Volunteer use and staff strategies in emergencies

Again, look to your HIPAA security program for parallels. Undoubtedly, you already have policies and procedures for your risk analysis, your contingency plan which includes your disaster recovery and emergency mode plan, and some sort of manner to contact key personnel in the case of an emergency. Look to your policies and procedures for training and testing of your contingency plan. Is it possible you have already documented procedures to evacuate your facility? How about your data backup plan? Will your policies and procedures to protect and/or recover your e-PHI help you meet the medical records preservation requirement?

The point I am making here is that there are similarities between the Emergency Preparedness Plan and your HIPAA security plan. So, as you work through your Emergency Preparedness Plan, keep in mind that you may already have some of the requirements in place through your HIPAA program and therefore, you won't have to "reinvent the wheel".

Hernan Serrano
HIPAA trek
hernan@hipaatrek.com