Codify
BY AAPC

Part B Insider (Multispecialty) Coding Alert

HIPAA: Are Your EHR-Contingency Plans HIPAA-Ready?

Consider these 5 HIPAA requirements when preparing for disaster.

A catastrophe is defined as an event causing great and often sudden damage. In the wake of such natural and manmade disasters, health care providers are usually the first on the scene, helping others, assessing the medical toil, and offering their crucial, timely care.

When chaos reigns during these tumultuous times, patients' safety and security are at their most vulnerable. Due to the indispensable and important role that the health care industry plays when the stakes are so high, it is essential that practices and hospitals alike put patients first when outlining a HIPAA-friendly, contingency plan.

Background. The Office of Civil Rights (OCR) requires that all covered entities have HIPAA-secure, contingency plans in place should calamities occur that may disrupt the integrity of EHRs. This HIPAA security rule specifies how the plan should be laid out to prepare for a variety of scenarios from natural disasters like flood or fire to disturbances caused by digital piracy.

After EHR issues accumulated with Superstorm Sandy and cyberattacks in a Boston hospital in 2014, the OIG felt more research needed to be done on the subject of HIPAA and contingency planning. "To gain a deeper knowledge of hospital EHR contingency plans and experiences, we also conducted site visits at six hospitals, where we interviewed hospital staff and reviewed EHR contingency plans and related documents," an OIG report published July 25, 2016 states.

Results. Extensive data garnered from the surveys sent out to 400 hospitals, which utilized certified EHRs, showed that about 95 percent had EHR contingency plans in place, the OIG report suggested. The questions dealt with how the hospitals integrated the five required HIPAA rules into their planning, whether or not they employed recommendations from the National Institute for Standards and Technology (NIST) and the ONC, and how staff members handled EHR disruptions.

What The Report Uncovered

The majority of those surveyed were addressing EHR issues with security and safety under duress, but many groups' contingency plans lacked the five necessary HIPAA requirements to make them complete. Unfortunately, the findings showed that because of the lack of some of these requirements, EHRs were disrupted and patient care was affected.

Five important rules. The OIG report maintains that every contingency plan must include five policies to make them HIPAA-compliant. All covered entities must include the following HIPAA fundamentals:

- A data back-up plan
- A disaster strategy for recovering lost data
- An operations plan that allows for business to continue during a state of practice or hospital emergency
- Audit and revision of plan to ensure that it works under pressure
- Critical assessment of all applications to address working order

Here Are Some Quick Tips to Help You Plan Accordingly

Luckily, the HHS, in coordination with the NIST and the ONC, offer help to providers seeking guidance when organizing a comprehensive, HIPAA-compliant contingency strategy. All three federal departments advise covered entities through a myriad offering of research, tools, and fact sheets.

If your practice is in the process of contingency planning, you might want to consider these ideas to make the ordeal

quick and easy.

Physician Approved

In addition to protecting your patients' rights under HIPAA in case of EHR failure, clinical matters should be addressed as well in regard to treatment and the disbursement of prescribed medicine.

Training and Practice

All staff must be aware of the possibility of disaster and what procedures to follow should the EHRs go down.

Back-up and Machinery

Not only should you ensure the proper back-up mechanisms for software and hardware, but it is also a good idea to investigate auxiliary equipment like a generator and extra fuel for emergency situations.

Communication and Audit

Keep the lines of communication open before, during, and after disaster strikes. This might be a secondary form of office communication that is practiced in case technology cannot be used. Also, test, revise, and audit your products and plans annually to ensure that everything and everyone is on the up and up.

Resources: For more information on the OIG study on EHRs and contingency planning, visit https://oig.hhs.gov/oei/reports/oei-01-14-00570.pdf.

To take a look at the ONC's contingency planning guide, visit https://www.healthit.gov/policy-researchers-implementers/safer/guide/sg003.

For the details from the NIST guidance on disaster planning, visit http://csrc.nist.gov/news_events/HIPAA-May2010_workshop/presentations/2-2b-contingency-planning-swanson-nist.pdf.