Health Information Compliance Alert

Information Security IT CONTINGENCY PLANS NEED 21ST CENTURY MAKEOVERS

Health care organizations need to do a better job thinking about the unthinkable and dust off those disaster recovery plans for their critical information systems.

While the Health Insurance Portability and Accountability Act's security rule has yet to be finalized, the proposed rule offers few specifics on contingency plans.

"There's just a basic requirement to maintain the integrity of systems," says Eddie Schwartz, senior vice president of professional services with Waltham, MA-based Guardent Inc. "You can create a plan that would meet the [HIPAA] requirements just by following a sort of best practice approach."

The lack of specific requirements for a contingency plan is by design, says C. Jon Burke, principal of HIPAAInfoTech in Anaheim, CA. "The rule is crafted in such a way as to prevent the obsoletism that occurs with standard disaster recovery plans."

But that flexibility has also caused "a rather large amount of confusion" for covered entities who would like a little more guidance in preparing for the worst, Burke adds.

Fortunately, the National Institute of Standards and Technology has just provided some of that guidance to organizations looking for best practices with the release of a document entitled the Contingency Planning Guide for Information Technology Systems.

According to the NIST, the seven stages of a contingency planning process are:

1. Develop a contingency planning policy. A formal department or agency policy provides the authority and guidance necessary to develop an effective contingency plan.
2. Conduct a business impact analysis (BIA). The BIA helps to identify and prioritize critical IT systems and components.
3. Identify preventive controls. Measures taken to reduce the effects of systems disruptions can increase system availability and reduce contingency life-cycle costs.
4. Develop recovery strategies. Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.
5. Develop the contingency plan. The contingency plan should contain detailed guidance and procedures for restoring a damaged system.
6. Test the plan and train the personnel. Testing the plan identifies planning gaps, whereas training prepares recovery personnel for plan activation; both activities improve plan effectiveness and overall agency preparedness.
7. Maintain the plan. The plan should be a living document that is updated regularly to remain current with system enhancements.

Though the NIST document offers general recommendations for all IT systems, Schwartz says it can be of particular benefit to health care organizations facing HIPAA security challenges.

Conducting the business impact analysis is vital. A covered entity can't know how much to spend on contingency planning by "reading a regulation or guessing what regulators are going to want to see," explains Schwartz. "It comes down to putting your own real value on your information assets."

For an effective BIA, covered entities will want to focus on two aspects of the systems and information they are protecting: criticality and sensitivity. The sensitive health information that HIPAA was drafted to protect should not

necessarily be the top priority when drafting a contingency plan. "The bottom line is that some systems that can be down for a couple of weeks and there are others that people don't want to see down for more than a couple of minutes," counsels Schwartz.

Simply having a disaster recovery plan on the shelf doesn't necessarily mean a covered entity is safe those plans must be dusted off and tested regularly. Many organizations find out when it's too late that their contingency planning was inadequate or outdated. "One of the things that I see is that people are still thinking in terms of the legacy models of disaster recovery," notes Schwartz.

Guard Against Old Thinking

In the past most information systems were designed around a central mainframe which made disaster recovery an expensive, but logistically simple operation. Today, however, most large information systems are complex and distributed, and therefore require much more in terms of contingency planning. "If you're using distributed systems or using the Internet or extranets for any technology delivery that's critical to your business, what you must do is think about the concept of 'fault resilience' where you're actually distributing the risk as well as distributing the systems." Larger companies should consider "server farms" or design their networks so that there is redundancy and load sharing.

Thinking in terms of older systems isn't the only problem disaster recovery planners run into some think only in terms of old disasters. "It's not just natural disasters, it's unnatural disasters," says Schwartz. Hackers, viruses and worms are probably more dangerous than fires or hurricanes and a good 21st century contingency plan should acknowledge that.

Burke agrees. "the biggest problems are caused when the plan itself is so rigorously structured that it can't flex with changes in the environment and changes in the threat condition."