Device Makers: Custodians of Patient Data

Charles Murphy, Vice President, Cloud Operations, Pilgrim Software

Q: As more medical devices collect patient data, what measures are being taken to secure the information and safeguard privacy?

The key to protecting PHI data is education, execution, and continuous verification. The first thing is to understand your obligation as a custodian of this sensitive data. This is best done through formal HIPAA/HIPAA-HITECH training to understand the regulation. Second, ensure that any custodial organization you involve has thorough and auditable security control standards in place to govern access and handling of sensitive data. The National Institute of Standards and Technology (NIST 800.xx) is a good example of such standards.

Once the controls are in place, internal and external audits of the controls and the controlled environment should be conducted on a recurring basis to ensure that the organization is following the documented controls. Next, the environment must be “hardened” and this should be verified by “penetration testing”—this too should happen as a recurring activity. An additional mandatory measure is to encrypt the PHI data, both during transmission and while “at rest.” “Data encryption at rest” is one way to seek “safe harbor” from a data breach. In the unfortunate event of a breach, the organization should have a well-documented incident handling and reporting process in place. An enterprise quality management system engineered for the life sciences industry will help organizations handle the incident with consistency and in a compliant manner. It will also secure the transmission of information and safeguard the privacy of the patient whether the information is being transmitted locally or through the cloud.

Source URL (retrieved on *04/16/2014 - 6:51am*):
http://www.mdtmag.com/blogs/2013/09/device-makers-custodians-patient-data