SHARING IN THE CARING

ASHRM

HRM WEEK

JUNE 16-20, 2014

E▪R▪M

HRM Week
Topic 2

Fighting on the Frontlines of Cyber Security

As healthcare embraces 21st Century technologies, the cyber security battles lines are drawn. With the tsunami of national retailers, corporations and the government being hacked, risk managers have every reason to feel inundated. It's even more daunting when you add to the scene evolving ePHI (electronic patient health information) requirements. However, there is an upside. The digital age brings the potential advantages of enhancing many aspects of healthcare including time efficiency, patient engagement, care coordination, record keeping and patient health information security. Unfortunately, the digital era has unleashed unparalleled cyber threats to security. The 2014 Verizon Data Breach Investigations Report examined some 63,000 security episodes and more than 1,300 breaches from 50 data-sharing partners. Healthcare was among the industries cited in the report as needing to increase security controls and expand measures.

Defending against cyber incursions and regulation infractions starts with identifying where vulnerabilities or impediments to achieving security might exist, such as:

- Multiple departments responsible for cyber security
- Overlapping or competing cyber security plans
- Frequently changing HIPAA, ePHI and other patient privacy directives or a lack thereof
- Unsecured and mishandled laptops and mobile devices
- Medical devices misfiring corrupting data and other equipment
- Insider misuse of health records information
- Inadvertent exposure of information
- Massive data files causing storage issues
- IT security errors by physicians and healthcare staff

Take these actions to achieve a solid cyber security system:

SHARING IN THE CARING

ASHRM

HRM WEEK

JUNE 16-20, 2014

E▪R▪M

HRM Week
Topic 2

Solutions:

- Gather a central cyber security team with scheduled frequent reporting updates and actions
- Create one clear, continually updated cyber security plan
- Implement a thorough cyber risk assessment review that includes digital devices and goes beyond checking off a list of HIPAA Security Rule and Meaningful Use requirements
- Establish a strict use policy for laptops and mobile devices including required encryption
- Audit and monitor those who access records to prevent misuse
- Implement quality sample processes (such as labels on envelopes or mass emails derived from records) so you can detect unwanted data before submitting
- Schedule systematic monitoring of the security firewalls and designations on Web or cloud-based data
- Consider cloud-based systems to enhance sharing capabilities and storage challenges
- Encourage physicians and staff to attend regular updates on proper procedures and solutions to new cyber threats

Individuals who may be involved in Cyber Security include:

- Risk managers
- Chief information officer
- Cyber security teams
- Health IT professionals and consultants
- Cyber security services
- Healthcare staff
- Physicians

For more information go to ashrm.org/hrmweek