Understanding the Stage 2 requirement to "Protect Electronic Health Information"

In the preamble of the Stage 2 Final Rule, CMS stated: "We did not propose to change the HIPAA Security Rule requirements, or require any more than is required under HIPAA. **We only emphasize the importance of an EP including in its security risk analysis an assessment of the reasonable and appropriateness of encrypting electronic protected health information (ePHI) as a means of securing it, and where it is not reasonable and appropriate, the adoption of an equivalent alternative measure.**"

Meaningful Use Stage 2 Objective "Protect Electronic Health Information" requires:

Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308 (a)(1), including addressing the encryption/security of data at rest and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.

1) Conduct or review a **security risk analysis**:
- **a)** Free risk assessment resources:
  - **i)** http://scap.nist.gov/hipaa/
  - **ii)** http://www.ohii.ca.gov/calohi/PrivacySecurity/ToolstoHelpYou/HIPAASecurityToolkit.aspx
- **b)** Have you identified where ePHI resides within your organization?
- **c)** What are the external sources of ePHI? For example, do vendors or consultants create, receive, maintain or transmit ePHI**?**
- **d)** What are the human, natural, and environmental threats to information systems that contain ePHI?
- **e)** What risks does the enhanced interoperability required in Stage 2 pose to your ePHI? Consider the following Stage 2 requirements:
  - **i)** Lab / Radiology Exchange: Lab results (>55%) and diagnostic images (>10%) are incorporated into the Certified Electronic Health Records Technology (CEHRT).
  - **ii)** Patient and Family Engagement: Patients (>50%) have online access to their ePHI within 4 business days, and patients or their authorized representatives (>5%) view, download, or transmit to a third party.
  - **iii)** Transitions of Care: Transitions of care and referrals (>50%) require a summary of care record. 10% are electronically transmitted using CEHRT and one or more exchanges are with a recipient using a different CEHRT.
  - **iv)** Public Health: Successful ongoing submission of electronic syndromic surveillance data, immunization data, or cancer case information from CEHRT to a public health agency or registry.

2) Address the **encryption/security of data at rest**:
- **a)** CMS added "data at rest" in Stage 2 to specify its inclusion of data that is stored in electronic health records systems and end-user devices.
- **b)** Have you made a determination of whether encryption is possible, and if not, do you have another means for protecting the ePHI at rest? Document the rationale for this determination.
- **c)** Have you included end-user devices such as laptops, tablets, and smart phones in your assessment of the appropriateness of encryption?

3) **Implement security updates** as necessary and **correct identified security deficiencies**:
- **a)** Determine the appropriate manner of protecting health information transmissions. (45 C.F.R. § 164.312(e)(1).)
- **b)** Decide whether and how to use encryption. (45 C.F.R. §§ 164.312(a)(2)(iv)and (e)(2)(ii).)
- **c)** Design appropriate personnel screening processes. (45 C.F.R. §164.308(a)(3)(ii)(B).)
- **d)** Identify what data to backup and how. (45 C.F.R. § 164.308(a)(7)(ii)(A).)
- **e)** Address what data must be authenticated in particular situations to protect data integrity. (45 C.F.R. § 164.312(c)(2).)

Lastly, while not specifically addressed in this meaningful use objective, EPs should consider communicating clearly to their patients the manner in which patient ePHI is being used and provide assurances that patient privacy is being protected.

HITEC-LA, a project of L.A. Care, is a federally-designated Regional Extension Center funded by the Office of the National Coordinator, Department of Health and Human Services, Award Number: 90RC0052/01