What's New with EHR Privacy and Security?

Trisha Harkness, CISSP, CHPS

Quality Forum

June 6, 2013

Accelerating aHIT
Health Information Technology in Kansas

kfmc Kansas Foundation for Medical Care, Inc.

Getting Interactive

Get ready to participate!

Need more caffeine?

Need to stretch?

Go for it!

Accelerating aHIT
Health Information Technology in Kansas

kfmc Kansas Foundation for Medical Care, Inc.

Getting Interactive

- True or False
  - Why?
- EHR software certified to ONC 2014 Edition standards and certification only affects eligible providers pursuing meaningful use.
  - False. Many vendors, in order to keep their marketability viable, will become certified. The 2014 Edition certification is an upgrade that will be installed by many physician clinics as part of their typical upgrade process.

Getting Interactive

- The addition of addressing the encryption and security of data stored in an EHR as part of the protection of electronic health information in Meaningful Use Stage 2 is to emphasize the importance of assessing the entity's potential need to encrypt the PHI to secure it.
  - True. The intention is to "emphasize the importance of an EP or hospital including in its security risk analysis an assessment of the reasonable and appropriateness of encrypting electronic protected health information as a means of securing it, and where it is not reasonable and appropriate, the adoption of an equivalent alternative measure".

Getting Interactive

- To attest to the meaningful use measure regarding protection of electronic health information, a security risk analysis must be conducted and the provider's risk management process must address discovered security deficiencies.
  - True. Please see CMS FAQ 7705 in the presentation slides.

https://questions.cms.gov/faq.php?id=5005&faqId=7705

Getting Interactive

- Since the US Postal Service and other couriers are merely conduits, it is recommended to send unencrypted PHI via those services.
  - False: All media containing electronic protected health information (ePHI) – whether USB drives, CDs/DVDs, backup tapes, etc. – shipped via courier services should be encrypted.
  - The decryption key should be shared with the ePHI recipient only via a different, secure transmission mechanism.

Getting Interactive

- If my online backup vendor receives my ePHI via a secure transmission and the ePHI at rest is encrypted with a key that is known only to the ePHI owner, the backup vendor is considered a conduit instead of a BA.
  - False. “[A]n entity that maintains protected health information on behalf of a covered entity is a business associate and not a conduit, even if the entity does not actually view the protected health information.”

Getting Interactive

- Every business associate subcontractor that has access to my PHI is liable under the HIPAA Rules.
  - True. “[U]nder the final rule, covered entities must ensure that they obtain satisfactory assurances required by the Rules from their business associates, and business associates must do the same with regard to subcontractors, and so on, no matter how far ‘‘down the chain’’ the information flows.”

Getting Interactive

- Both new and existing BA Agreements have a transition period deadline of September 22, 2014.
  - False: "The additional transition period would be available to a covered entity or business associate if, prior to the publication date of the modified Rules, the covered entity or business associate had an existing contract or other ***written*** arrangement with a business associate or subcontractor, respectively, that complied with the prior provisions of the HIPAA Rules and such contract or arrangement was not renewed or modified between the effective date and the compliance date of the modifications to the Rules." (Emphasis added.)

Federal Register, Vol. 78, No. 17, Page 5603

Getting Interactive

- The loss of unsecured electronic media containing 505 patient records would be considered a single violation.
  - False: Where multiple individuals are affected by an impermissible use or disclosure, it is anticipated that the number of identical violations would be counted by the number of individuals affected.
  - "In the case of continuing violation of a provision, a separate violation occurs each day the covered entity or business associate is in violation of the provision."
  - When calculating the civil money penalty, consideration factors include "[t]he nature and extent of the violation, consideration of which may include but is not limited to:
    (1) The number of individuals affected; and
    (2) The time period during which the violation occurred"

Federal Register, Vol. 78, No. 17, Page 5584 and 5691

Getting Interactive

- The maximum penalty for HIPAA violations for a given calendar year can exceed $1,500,000.
  - True: “In many breach cases, there will be both an impermissible use or disclosure, as well as a safeguards violation, for each of which the Department may calculate a separate civil money penalty.”
  - “One covered entity or business associate may be subject to multiple violations of up to a $1.5 million cap for each violation, which would result in a total penalty above $1.5 million.”

Federal Register, Vol. 78, No. 17, Page 5584

Getting Interactive

- Penalty example for loss of unsecured electronic media containing 505 patient records
  - Impermissible disclosure violations
    - Reasonable Cause (2): $1,000 x 505 records = $505,000
    - Willful Neglect (3): $10,000 x 505 records = $5,050,000
      - Cap of $1,500,000 would be assessed.
  - Failure to properly address encryption of electronic media for 90 days from date of violations
    - Reasonable Cause (2): $1,000 x 90 days = $90,000
    - Willful Neglect (3): $10,000 x 90 days = $900,000
  - Total penalty for violations of both HIPAA provisions
    - Reasonable Cause (2): $505,000 + $90,000 = $595,000
    - Willful Neglect (3): $1,500,000 + $900,000 = $2,400,000

Getting Interactive

- Since a business associate is now directly liable for civil money penalties assessed on HIPAA violations, covered entities do not need to monitor BA's HIPAA compliance.
  - False. "A covered entity is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the covered entity, including a workforce member ***or business associate***, acting within the scope of the agency". (Emphasis added)

Getting Interactive

- My contracted data destruction company needs to comply with Privacy Rules related to non-disclosure of PHI and document destruction, Security Rules related to media disposal, and general Security Administrative Safeguards.
  - True. “[S]ome business associates … may not have engaged in the formal administrative safeguards such as having performed a risk analysis, established a risk management program, or designated a security official, and may not have written policies and procedures, conducted employee training, or documented compliance as the statute and these regulations would now require.”

Federal Register, Vol. 78, No. 17, Page 5589

Getting Interactive

- Business Associate liability for impermissible uses and disclosures of PHI under the HIPAA Privacy Rule attaches upon execution of the business associate contract or agreement.
  - False. “[L]iability for impermissible uses and disclosures attaches immediately when a person creates, receives, maintains, or transmits protected health information on behalf of a covered entity or business associate and otherwise meets the definition of a business associate.”

For More Information Contact

Trisha Harkness, CISSP, CHPS
Kansas Foundation for Medical Care, Inc.
2947 SW Wanamaker Dr.
Topeka, KS 66610
Email: tharkness@kfmc.org
Phone: (620) 874-8034
Linked In:
http://www.linkedin.com/pub/trish-harkness/5/b3/410/

This material was prepared by Kansas Foundation for Medical Care, Inc. as part of our work as the Kansas Regional Extension Center, under grant #90RC00031/01 from the Office of the National Coordinator, Department of Health & Human Services. RC_2013_12