Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

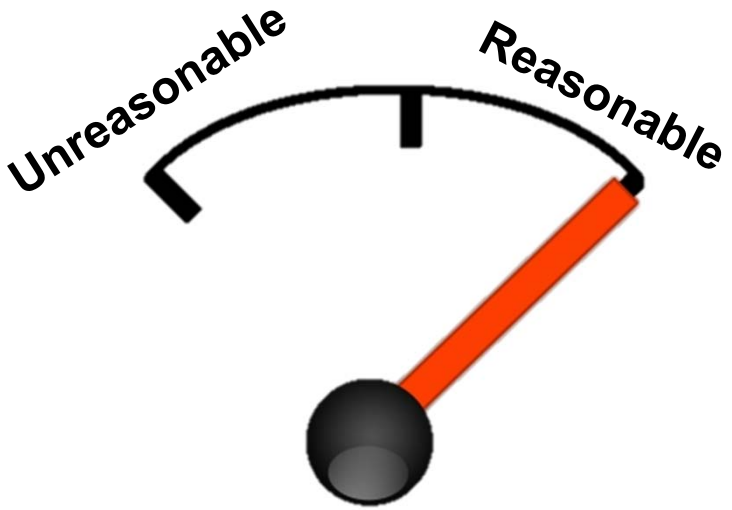
Meaningful Use Crosswalk to the Security Rule

Safeguarding Health Information: Building Assurance through HIPAA Security
June 7, 2012

Adam H. Greene, J.D., M.P.H.
Partner, Davis Wright Tremaine

EHR Certification Criteria

- Certified EHR technology must have certain privacy and security functionalities
- MU does not require the use of most of those functionalities, but …
- Availability of functionalities affects what is "reasonable and appropriate" under HIPAA Security Rule



Current EHR Certification Criteria

- Access control
  - Assign unique IDs and establish controls to limit unauthorized access
  - 45 CFR 164.312(a)(1)
- Emergency access
  - 45 CFR 164.312(a)(2)(ii)

Current EHR Certification Criteria

- Automatic log-off
  - 45 CFR 164.312(a)(2)(iii)
- Accounting of disclosures (optional)
  - 45 CFR 164.312(b) (audit controls)

Current EHR Certification Criteria

- Authentication
  - 45 CFR 164.312(d)
- Integrity
  - 45 CFR 164.312(e)(2)(i)
  - Create a message digest
  - Verify integrity upon receipt
- Encryption when exchanging information
  - 45 CFR 164.312(e)(2)(ii)

Revised 2014 EHR Certification Criteria

- Audit logs
  - 45 CFR 164.312(b)
  - Turned ON as default,
    - Ability to turn off audit log limited to certain designated persons (e.g., system administrator)
  - Record actions related to ePHI, audit log status, and encryption of end-user devices
  - Records cannot be changed, overwritten, or deleted
  - Detect alteration of audit logs
  - Create audit logs

Revised 2014 EHR Certification Criteria

- Encryption of data at rest
  - 45 CFR 164.312(a)(iv)
  - Electronic health information store on end-user devices is encrypted after use of EHR is stopped; or
  - Ensure EHI never remains on end-user device after use of EHR is stopped

New 2014 EHR Certification Criteria

- Secure messaging for ambulatory systems
  - Not restricted to email; may include patient portal, PHR, or other messaging system
  - Adopts encryption and hashing algorithm standards as baseline
- Amendments
  - Allow user to amend patient's health record
  - Append patient supplied information and response to same

MU Stage 2 Objective: View Online, Download and Transmit

- Provide patients the ability to view online, download and transmit their health information to third parties
  - >50% patients have access
    - EPs – within 4 business days
    - Hospitals – within 36 hours of discharge,
  - >10% of patients view, download or transmit
- Replaces and consolidates e-copy and online access objectives from Stage 1

Portals and Security

- Risk analysis and Risk management (45 C.F.R. 164.308(a)(1)(ii)(A) and (B))
  - What is risk of interception in transit?
  - What is risk that portal user is not authorized user?
  - What is risk that information is corrupted in transit?

Portals and Security

- Integrity (45 CFR 164.312(e)(2)(i))
  - Is the it reasonable to ensure that information is not modified or destroyed during transmission?
- Encryption (45 CFR 164.312(e)(2)(ii))
  - Is it reasonable and appropriate to encrypt the portal information in transit?
- Unique user IDs (45 CFR 164.312(a)(2)(i))
  - Should family or friends get separate IDs?

Portals and Security

- Authentication (45 CFR 164.312(d))
  - Implement procedure to verify identity
  - What is reasonable and appropriate for patients?
- Audit logs (45 CFR 164.312(b))
- Review of audit logs (45 CFR 164.308(a)(1)(D))
- CE is not responsible for information on patient's end

MU Stage 2 Objective: Send Patient Reminders (EPs)

- Measure:
  - >10% of patients who visited EP within past 24 months
  - Send a reminder per patient preference
- Patient preference refers to method of transmission
  - Not inquiry as to whether they would like to get reminders

MU Stage 2 Objective: Send Patient Reminders (EPs)

- Step 1 – Reasonable and appropriate safeguards
  - Encryption?
  - Correct address?
- Step 2 – Accomodate reasonable patient requests
  - Patient may prefer unencrypted e-mails

MU Stage 2 Objective: Secure Electronic Messaging (EPs)

- Measure:
  - >10% of patients send secure electronic message to EP

- Not limited to email; could include communications through patient portal, PHR or other messaging application

Secure Messaging with Patients

- MU focuses on patient-initiated communications, while HIPAA focuses on provider-initiated communications
- Provider-initiated communications should be addressed in risk analysis
  - Consider likelihood of risk (e.g., interception, misdirection)
  - Consider impact of risk (may vary based on content)
- Some communications may not require “secure” system

MU Stage 2: Electronic Health Information Exchange

- Immunization data to immunization registry or information system (EPs and Hospitals -- Core)
- Lab results to public health agencies (Hospitals only -- Core)
- Syndromic surveillance data to public health agencies (Hospitals -- Core; EPs -- Menu)
- Cancer case information to cancer registry (EPs – Menu)
- Case information to a specialized registry (EPs – Menu)

MU Stage 2: Electronic Health Information Exchange

- Partnering with HIE organizations
  - HIEs may transport data on behalf of public health agencies
    - Cannot transform content or message
  - HIEs may serve as extension of CEHRT for providers
    - Must be certified for relevant EHR certification criteria in accordance with certification program
- Must use transport standard supported by public health agency

Security and HIE

- Have potential threats and vulnerabilities been addressed in risk analysis?
- Is transmission encrypted if reasonable and appropriate?
- If partnering with HIE, is business associate agreement in place?
  - Does BA contract permit disclosure to public health authorities?

MU Stage 2 Objective: Provide Summary of Care Record

- Exchange key clinical information during transitions of care
  - Replaces “electronic exchange of health information”
- Two measures to meet objective:
  - Provide a summary of care for >65% of transition of care and referrals; and
  - Electronically transmit summary of care for >10% of transitions of care and referrals, where
    - Recipient has no organizational affiliation; and
    - Recipient using a different CEHRT

Security and HIE

- Have potential threats and vulnerabilities been addressed in risk analysis?
  - Is transmission encrypted if reasonable and appropriate?
  - Are systems in place to avoid misdirection?
- Exchange between different systems may increase risks
- CE is not responsible for security of recipient

Stage 2 MU:
Electronic Medication Administration Record

- New core objective for hospitals
  - Automatically documents the administration of medication into CEHRT using electronic tracking sensors
- Electronic verification before administering medication
  - Right patient
  - Right medication
  - Right dose
  - Right route
- Electronically record when and who administers

eMAR and HIPAA

- Is new ePHI related to eMAR included in risk assessment (including any ePHI that resides on devices)?
  - What are the threats and vulnerabilities (e.g., loss of devices, interception of transmissions)?
  - Are all risks managed to a reasonable and appropriate level?
- Is information encrypted if reasonable and appropriate? (at rest and in transit)

MU Stage 2: Protect Electronic Health Information

- Measure: Conduct or review a security risk analysis in accordance with requirements of HIPAA Security Rule
  - Specifically requires addressing encryption/security of data at rest
    - Does not require use of encryption, but assessment of data security at rest
    - Not limited to data at rest
  - Must also implement security updates and correct deficiencies

- Review must be updated for each reporting period
  - Becomes annual update process to meet MU annually

Risk Analysis Under MU & HIPAA

- Risk Analysis is required under both MU and HIPAA
  - HIPAA requires risk analysis for all PHI, not just EHR
- MU Stage 2 measure emphasizes analysis of encryption of EHR data at rest
  - Under HIPAA, also don't forget about non-EHR on mobile devices
- Bottom line: COMPLY WITH HIPAA SECURITY RULE

For more information

Adam H. Greene, JD, MPH

Davis Wright Tremaine LLP

adar[illegible]

202.973.4213

Questions