Today’s Panel

Jane Eckels, JD
Davis Wright Tremaine
jane.eckels@dwt.com
206.757.8037

Adam H. Greene, JD, MPH
Davis Wright Tremaine
adam.greene@dwt.com
202.973.4213

Kurt J. Long
FairWarning® Founder and CEO
Today’s Agenda

Meaningful Use Stage 2 & HIPAA: The Relationship Between HIPAA and Meaningful Use Privacy & Security Regulations

- Adjusting HIPAA Compliance to Meet the Stage 2 Meaningful Use Proposal
  - EHR Certification Criteria
  - EHR Portals
  - Patient Reminders
  - Secure Messaging
  - Electronic Health Information Exchange
  - Clinical Decision Support
  - Electronic Medication Administration Records
  - Security Risk Assessment

- Meaningful Use and Audit Controls

- Q&A Session
Adjusting HIPAA Compliance to Meet the Stage 2 Meaningful Use Proposal

Jane Eckels, JD
Partner
Davis Wright Tremaine

Adam Greene, JD, MPH
Partner
Davis Wright Tremaine
Agenda

- EHR Certification Criteria
- EHR Portals
- Patient Reminders
- Secure Messaging
- Electronic Health Information Exchange
- Clinical Decision Support
- Electronic Medication Administration Records
- Security Risk Assessment
“2014 Edition” EHR Certification Criteria

- **New privacy and security criteria include:**
  - Secure messaging for ambulatory systems
  - Amendments

- **Revised privacy and security criteria include:**
  - Auditable events and tamper resistance
  - Audit reports
  - Encryption of data at rest

- **Unchanged privacy and security criteria include:**
  - Authentication, access control & authorization
  - Accounting of disclosures
  - Automatic log-off
  - Emergency access
  - Integrity
“2014 Edition” EHR Certification Criteria

- **Amendment**
  - Allow user to amend patient’s health record
  - Append patient supplied information and response to same

- **Secure Messaging**
  - Not restricted to email; may include patient portal, PHR, or other messaging system
  - Adopts encryption and hashing algorithm standards as baseline
“2014 Edition” EHR Certification Criteria

- **Audit**: more stringent audit logs to better detect and investigate breaches:
  - Audit log must be:
    - Turned ON as default,
    - Immutable,
    - Record action occurred, and
    - Specific e-health info to which the action applies
  - Records when and who turns OFF the audit log
    - Ability to turn off audit log limited to certain designated persons (e.g., system administrator)
  - Records when and who turns encryption OFF

- **Encryption of Data at Rest**: 2 ways to meet to meet criterion
  - 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
EHR Certification Criteria

- MU generally does not require use of CEHRT privacy and security capabilities, but...
- Availability of features affects what is “reasonable and appropriate” under HIPAA
- Many CEHRT features provide improved privacy and security capabilities, but...
- CEHRT is designed primarily for MU, not HIPAA compliance
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

- **Two measures to meet objective:**
  - Greater than 50% of patients are provided timely online access
    - EPs – within 4 business days of information being available to EP;
    - Hospitals – within 36 hours of discharge,
  - Greater than 10% of patients (or their authorized representatives) view, download or transmit
    - Requires patient activity

- Replaces and consolidates e-copy and online access objectives from Stage 1
MU Stage 2 Objective: View Online, Download and Transmit

- Does not require ALL EHR information to be accessible online
  - Covers a set of basic information
  - Minimum information is a list of specific data maintained in the CEHRT
  - May, but not required, to make more information available

- EPs have discretion to withhold information if its disclosure would cause substantial harm to patient
  - Ability to withhold applies to MU objective
  - Does not override obligation to allow individual to inspect and obtain copy of PHI in a designated record set
Online Patient Access to Records

- Providing MU online access ≠ HIPAA compliance
  - Patient is entitled to greater amount of PHI under HIPAA (designated record set) than EHR
  - Patient is entitled to requested form and format if readily producible, e.g., may have online access but want to receive PHI in another form (e.g., hard copy)
Online Patient Access to Records

- MU has much shorter time frames
  - MU: 50% of patients must have access within 4 business days of availability (EP) or 36 hours of discharge (EH) (regardless of whether they seek the information)
  - HIPAA: 100% of patients must receive PHI within 30/60 days of request (30-day extension available)
Online Patient Access to Records

- What happens to grounds for denial?
  - Psychotherapy notes
  - For criminal, civil, or administrative proceeding
  - Prohibited by CLIA
  - Corrections institute
  - Clinical research
  - Prohibited by Privacy Act
  - Likely to endanger individual or other
  - References another and likely to cause harm to other
  - Request is by personal representative and access could cause harm
Online Patient Access to Records

Online portal should be limited to:

- Patient
- Personal representatives
  - May need documentation of authority
  - Authority may change over time
- Persons identified by the individual as involved in care
  - Opportunity to agree/object required
  - PHI must be relevant to person’s involvement
- Others identified by HIPAA-compliant authorizations
  - Authorization may expire
- Other Designees? (HIPAA proposal)
Online Patient Access to Records

- Access to minors’ records raises challenges
  - Personal-representative status changes with age of majority
  - Guidance indicates that CE may rely on authorization by personal representative even after minor reaches age of majority

- Limited amount of disclosable PHI raises challenges
  - Some health information may not be disclosable to personal representatives (e.g., parents)
  - Limiting PHI to involvement in care/payment may not be feasible
Portals and Security

- What threats and vulnerabilities are created through portal access? Consider addressing in risk analysis.

- Is transmission encrypted?

- Is authentication reasonable and appropriate?
  - Are strong passwords required?
  - Is there a limit on failed login attempts?

- Is access to the portal logged and reviewed?
MU Stage 2 Objective: Send Patient Reminders (EPs)

- **Measure:**
  - Greater than 10% of unique patients who had an office visit with EP within 24 months prior to beginning of the EHR reporting period
  - Sent 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)

- EPs meet the “per patient preference” requirement if they accommodate patient requests per 45 CFR 164.522(b)

- Compliance with the guidance established under HIPAA for accommodating patient requests satisfies this requirement
Patient Reminders and HIPAA

- HIPAA requires provider to accommodate reasonable requests to receive communications by alternative means or at alternative locations.

- MU fits well with HIPAA due to recognition of patient preference.

- HHS guidance suggests that unencrypted e-mails for reminders may be permissible if consistent with patient preference.
MU Stage 2 Objective: Secure Electronic Messaging (EPs)

- **Measure**: greater than 10% of patients seen by the EP during the reporting period send secure electronic message to EP
  - Requires patient action; measured by *patient-sent email* in order for EP to meet measure
  - Expected to contain relevant health information, but does not look at content
  - EP response expected, but not measured

- Not limited to email; CEHRT 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 Public Health Objectives: Electronic Health Information Exchange

- Public health objectives require electronic transmission of health information to public health agencies (PHAs), except where prohibited, and in accordance with applicable law and practice
  - Submit electronic immunization data to immunization registry or information system (EPs and Hospitals -- Core)
  - Submit electronic reportable lab results to public health agencies (Hospitals only -- Core)
  - Submit electronic syndromic surveillance data to public health agencies (Hospitals -- Core; EPs -- Menu)
  - Identify and report cancer case information to cancer registry (EPs -- Menu)
  - Identify and report specific case information to a specialized registry (EPs -- Menu)

- **Measure:** Ongoing submission of relevant electronic health information for entire EHR reporting period
  - Unlike Stage 1, failed submission will not meet measure
MU Stage 2 Objective: 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

- Expecting public health agencies to supply providers with letter affirming submission of relevant information
Do all disclosures comply with Privacy Rule?
- To a “public health authority”?
- Minimum necessary?

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 Care Coordination Objective: Provide Summary of Care Record

- Exchange key clinical information during transitions of care and referrals
  - Replaces and consolidates Stage 1 “exchange of key clinical health information” and “provide summary of care record”

- Two measures to meet objective:
  - Provide a summary of care for greater than 65% of transition of care and referrals; and
  - Electronically transmit summary of care for greater than 10% of transitions of care and referrals, where
    - Recipient has no organizational affiliation; and
    - Recipient using a different CEHRT
  - Unlike Stage 2, unsuccessful test is not sufficient
Health Information Exchange: Treatment

- Will not be subject to minimum necessary standard because for treatment

- Patient can request restriction (e.g., opt-out), but provider not required to agree

- Have potential threats and vulnerabilities been addressed in risk analysis?

- Is transmission encrypted if reasonable and appropriate?
Stage 2 MU Objective: Clinical Decision Support

- Increased use of CDS in Stage 2

  2 Measures:
  - Implement 5 clinical decision support interventions related to 5 or more CQMs
  - Enable and implement functionality for drug-drug and drug-allergy interaction checks

- CEHRT CDS capability will allow providers to see:
  - Developer of intervention
  - Bibliographic citation
  - Funding source of intervention
  - Release/revision date of intervention
Clinical Decision Support & HIPAA

- Are CDS alerts part of the designated record set?
  - Is it health information?
  - Is it individually identifiable?
  - Is it used, in whole or in part, by the covered entity to make decisions about the individual?
  - The term “record” ... connotes information that has been recorded in some manner. (HHS guidance)

- There may be far better reasons then HIPAA to record and provide CDS information to patients as part of medical record.
Stage 2 MU Objective:
Electronic Medication Administration Record (EHs and CAHs)

- New core objective for hospitals
- Defined for MU as technology that 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 Objective: 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 conducted for each reporting period
  - Becomes annual process to meet MU annually
Risk Analysis Under MU & HIPAA

- Risk Analysis is required under both MU and HIPAA
  - Unclear whether MU requirement applies beyond EHR
  - HIPAA clearly requires risk analysis for all PHI

- MU Stage 2 measure emphasizes analysis of encryption of EHR data at rest
  - Under HIPAA, don’t forget about non-EHR on mobile devices

- Bottom line: COMPLY WITH HIPAA SECURITY RULE
Meaningful Use and Audit Controls

April 12, 2012
HIPAA Compliance is Dependent on Audit Logs

Regulatory responsibilities dependent on audit logs of systems that access ePHI.

- **Audit Controls**: HIPAA Security Technical Safeguards
- **Information Systems**: Activity Review HIPAA Security Admin. Safeguards
- **Mitigation**: Privacy Rule Admin. Safeguards

Accounting of Disclosures Rule Access Report pending
Pragmatic Challenges of Complying with HIPAA

- Audit logs may be unavailable or inadequate
- Systems may not be sized for auditing, so disabled
- Vendors charge a fee to enable logging
- Vendors may generate audit logs on complaint basis only
- Vendor enable logging but charges a fee to decipher / decrypt
- Lack of audit log integrity against errors and bad-actors
  - Unprotected
  - Overwrite
  - No retention plan
  - Changes undetected
Meaningful Use Stage 1

- Certified EHRs must produce audit log
- Specification of required data elements
- Human readable form
Meaningful Use Stage 2

- EHR audit logging must be enabled by default

- EHR audit log integrity
  - Tamper proof
  - Alterations detected
  - NTP and event ordering
  - Controlled administration for enabling & disabling

- Patient portal access review
# HIPAA, MU Stage 1 & Stage 2

Firm Foundation for Audit Controls

<table>
<thead>
<tr>
<th>Certification Criteria (EHRs)</th>
<th>Addresses</th>
<th>FairWarning®</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Meaningful Use Certification Criteria Stage 1</strong></td>
<td>General availability EHR audit logs</td>
<td>Immediately compatible with audit logs certified EHRs</td>
</tr>
<tr>
<td>Certified EHRs shall produce an audit log</td>
<td>Usefulness of content in EHR audit logs</td>
<td>Over 170 EHRs &amp; applications supported and in production</td>
</tr>
<tr>
<td>Specification of required data elements</td>
<td>EHR / application vendor practices</td>
<td>FairWarning® Data Definition Guide</td>
</tr>
<tr>
<td>Human readable form</td>
<td>Charging for deciphering / decrypting</td>
<td>Conformance with RFC: 3881, HL7, ATNA, DICOM</td>
</tr>
<tr>
<td>Time &amp; user sorted report</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Meaningful Use Certification Criteria Stage 2</strong></td>
<td>EHR / application vendor practices</td>
<td>Creates tamper-proof, forensically sound repository of audit logs.</td>
</tr>
<tr>
<td>Enabled by default</td>
<td>Default is “on”</td>
<td>Create chain of custody for handling of audit data</td>
</tr>
<tr>
<td>Administrative user control with on/off recorded</td>
<td>Systems sizing for auditing</td>
<td>Exceeds FIPS requirements</td>
</tr>
<tr>
<td>Audit log protection</td>
<td>Forensic evidence ready</td>
<td>Conforms to NTP</td>
</tr>
<tr>
<td>Conforms to FIPS</td>
<td>Logging of “view-only” transactions</td>
<td>Detection of alteration of all audit logs from MU certified and applications</td>
</tr>
<tr>
<td>NTP and event ordering</td>
<td></td>
<td>that access ePHI</td>
</tr>
<tr>
<td>Detection of the alteration of audit logs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User actions in EHR defined</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Meaningful Use Certification Criteria Stage 2</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient portal access review</td>
<td>New</td>
<td>Immediately compatible and available for review</td>
</tr>
<tr>
<td><strong>Meaningful Use Certification Criteria Stage 2</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient portal access review</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Stage 1 & 2 Establishes Firm Foundation for Audit Controls

Systems that access ePHI.
Examples: Revenue Management, PACS, Registration, etc.

MU Certified
Logs available with minimum fields; logs protected and enabled by default.
Privacy Monitoring & Breach Detection

- Full featured turn-key solution
  - Patient and user investigations
  - Proactive alerting with filtering
  - Ad hoc access reporting
  - Incident tracking and reporting
  - Zero FTE system operation requirement

- 170+ Production supported EHRs and healthcare applications

- FairWarning® invented and leads the category, reference KLAS Research, Gartner

- Over 160 customers representing over 800 leading hospitals
Audit Controls HIPAA Readiness

Best practices white paper and evaluation guide

Download here, full URL below:

Today’s Panel

Jane Eckels, JD
Davis Wright Tremaine
janebeckels@dwt.com
206.757.8037

Adam H. Greene, JD, MPH
Davis Wright Tremaine
adamgreene@dwt.com
202.973.4213

Kurt J. Long
FairWarning® Founder and CEO