Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

KAISER PERMANENTE

A Plan of Attack for Covered Entities: Steps to Comply with HIPAA 2.0

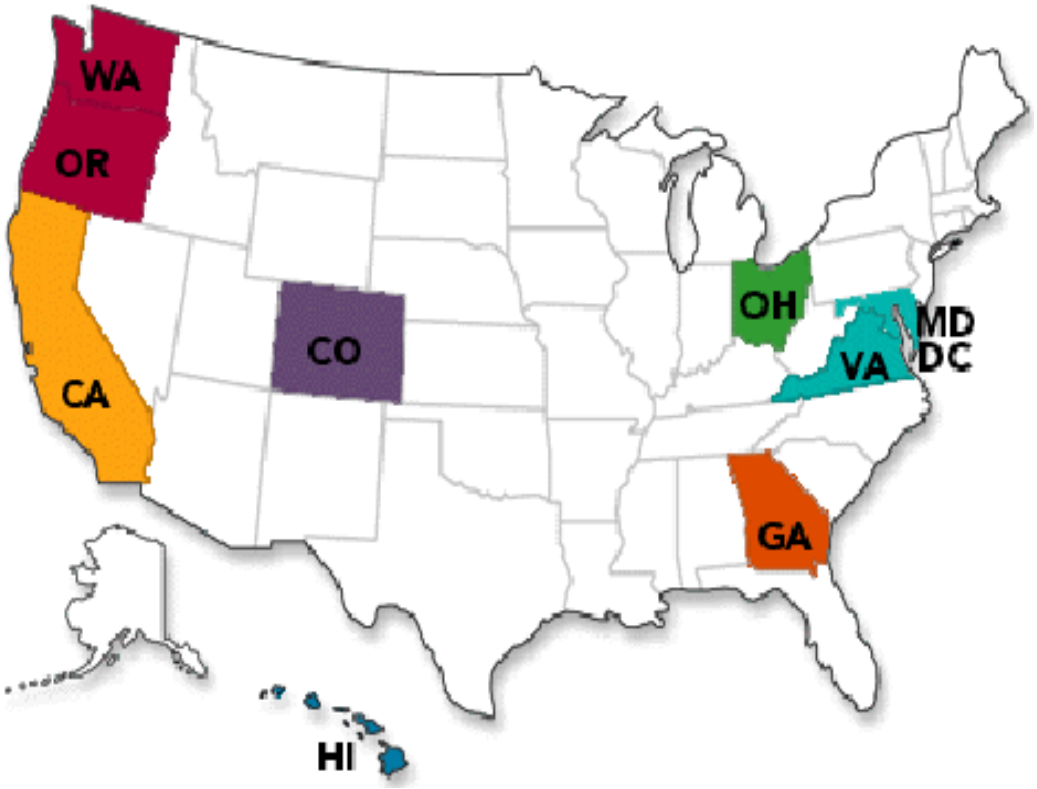
The Twenty-First National HIPAA Summit
February 19, 2013

Adam H. Greene, JD, MPH
Davis Wright Tremaine LLP

Yuan Y. Chen, JD
Kaiser Permanente

Kaiser Permanente Structure

Privacy & Security



Kaiser Permanente

- Nation's largest not-for-profit health plan, 9 million members
- Integrated health care delivery system
- 37 hospitals
- 611 medical offices and other outpatient facilities
- 16,658 physicians
- 172,997 employees
- 365 outpatient pharmacies

Structure, Privacy & Security

- Regional Privacy & Security Officer
- National Privacy & Security Officer

Policies and Procedures

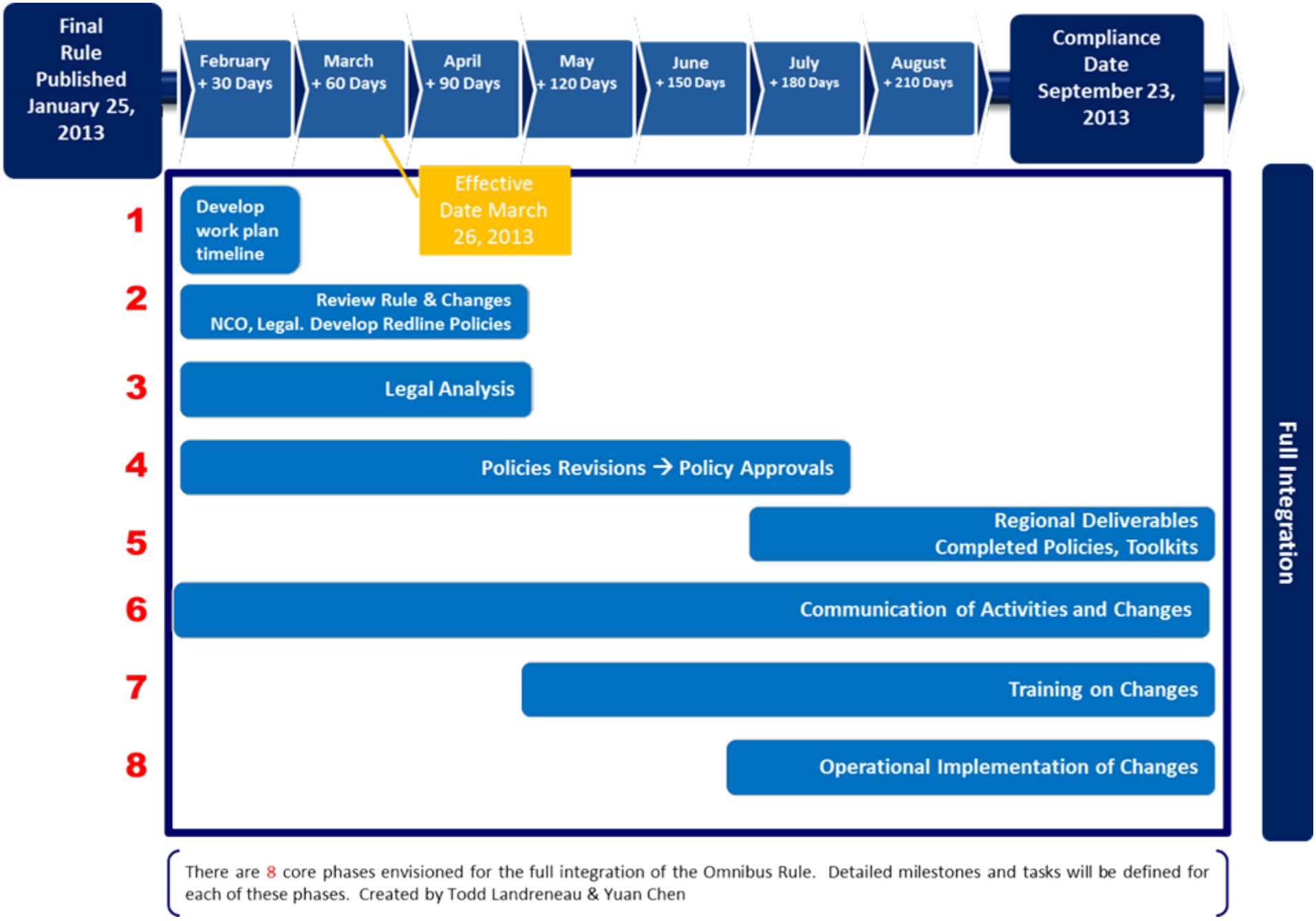
- Revisions to Policies and Procedures
  - Breach notification
  - Use and disclosure of PHI for marketing
  - Sale of PHI
  - Electronic access to designated record set
  - Requests for restrictions
  - Notice of privacy practices

Policies and Procedures

- Revisions to Policies and Procedures
  - Use and disclosure of decedent information
  - Fundraising
  - Authorization for use and disclosure for research
  - Student immunization records
  - Use of PHI for underwriting (health plans)

Policies and Procedures

- Other Policies to Revisit
  - Mobile devices (both enterprise-owned and personal devices)
  - Social media
  - Disposal



There are 8 core phases envisioned for the full integration of the Omnibus Rule. Detailed milestones and tasks will be defined for each of these phases. Created by Todd Landreneau & Yuan Chen

Training

If you draft or revise a policy, but do not train anyone on it, does it make a sound?

Training

- Develop a strategic plan for training
  - Cover changes from Omnibus Rule
  - Cover high-risk areas such as mobile devices and social media
- Consider breaking up training
  - Uses and disclosures
  - Safeguards
  - Patient privacy rights
  - Breach notification

Training

- Consider multiple training platforms
  - E.g., include as agenda item in departmental meeting
  - Make sure there is always documentation
- Don’t try to make workforce into HIPAA experts

Kaiser Permanente Training Plan

- Annual compliance training
  - Privacy policies as well as ethics
  - General training for entire workforce
- Omnibus communication plan
  - Changes to operations
  - Creation of toolkits and summaries
  - Make it easy

Breach Notification

- Policies and procedures
- Integrate changes to harm threshold
  - Low probability of compromise standard
  - Four required risk assessment factors
- Focus on objective and well-documented response program

Kaiser Permanente Breach Notification

- Impact of change from harm standard to presumption
  - OCR
  - Covered entities
- State law integration
- Heightened awareness of privacy rights
  - Impact on breach notification

Business Associates

- Inventory of business associate agreements
  - Have you recognized all business associates?
  - Do you have BAAs with non-business associates?
- Consideration of agency relationship
  - Timeframe for breach notification
  - Monitoring of BA

Business Associates

- Revisions to agreements
  - Breach notification (citing 164.410 vs. spelling out timing and content)
  - Specifying HITECH provisions (e.g., sale of PHI) vs. relying on general provision (BA shall comply with HIPAA)
  - Delegation of covered entity obligations

Business Associates

- Revisions to agreements
  - Additional clarity regarding subcontractors?
  - Clarity regarding minimum necessary?
  - Delegation of covered entity obligations?
  - More detailed safeguard requirements?
  - Revisit indemnification?

Kaiser Permanente Business Associates

- Significant number of vendors
- Revision of business associate agreement
  - Change in practices will require ramp-up time
- Auditing your business associates
  - Feasibility
  - Desk assessments

Notice of Privacy Practices

- Prohibition on sale of PHI
- Duty to notify affected individuals of a breach of unsecured PHI
- Right to opt out of fundraising (if applicable)
- Right to restrict disclosure of PHI when paid out of pocket
- Limit on use of genetic information (certain health plans only)
- Kaiser Permanente
  - Cost and Resources

Auditing

- Avoiding “willful neglect”
  - What policies and procedures are not working?
  - Do people know what they need to do?
- Minimizing breaches
  - Do you know where PHI is going?
  - Should there be auditing of business associates?

Auditing

- Audit Readiness
  - Creating tools for self-assessment
  - Focus on top areas outlined by OCR in past talks on areas needing improvement

For more information…

Adam H. Greene, JD, MPH

Davis Wright Tremaine LLP

adamgreene@dwt.com
202.973.4213

Yuan Y. Chen, JD

KAISER PERMANENTE

Yuan.Y.Chen@kp.org
626.405.6665

Questions