Compliance Challenges: Those Nagging Issues That Don't Seem to Go Away

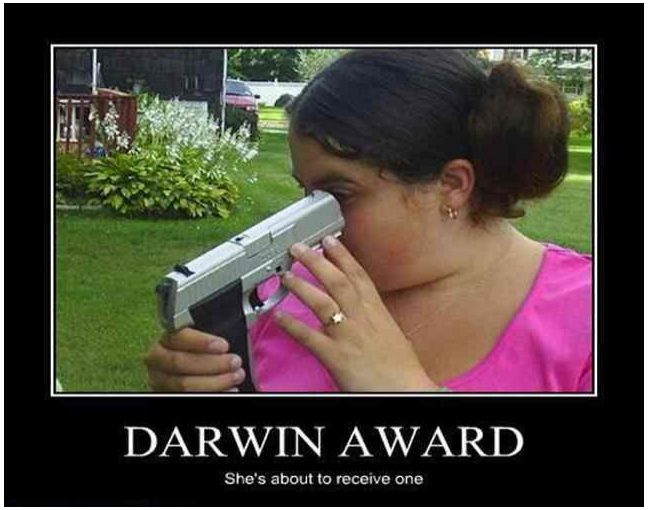
Lyra Correa, JD
Associate, Davis Wright Tremaine LLP
Washington, DC
lyracorrea@dwt.com

Davis Wright Tremaine LLP

HIPAA Roulette

The Human Factor

- Privacy and security are only as strong as your weakest link
- People often are the weakest link
  - Social engineering
  - Curiosity
  - Financial gain
  - Malice



The Human Factor

- "Ex-Factor" -- Top risks for intentional misuse, improper disclosures, and false accusations:
  - Ex-relationships: divorces, custody disputes, break-ups, new significant others, and so on
  - Ex-employees
  - Even ex-classmates (e.g., high school grudges)
- Other high-level risks include:
  - Friends and family
  - Co-workers
  - Celebrities of one form or another

The Human Factor: Action Steps

- When there is “history,” dig a little deeper
  - Could go either way
- Clear policies
- Train
- Culture of Compliance
  - Emphasize: Think before you click
- Audit records of patients who may be temptations
- Revisit sanction processes
- Apply sanctions in a consistent manner

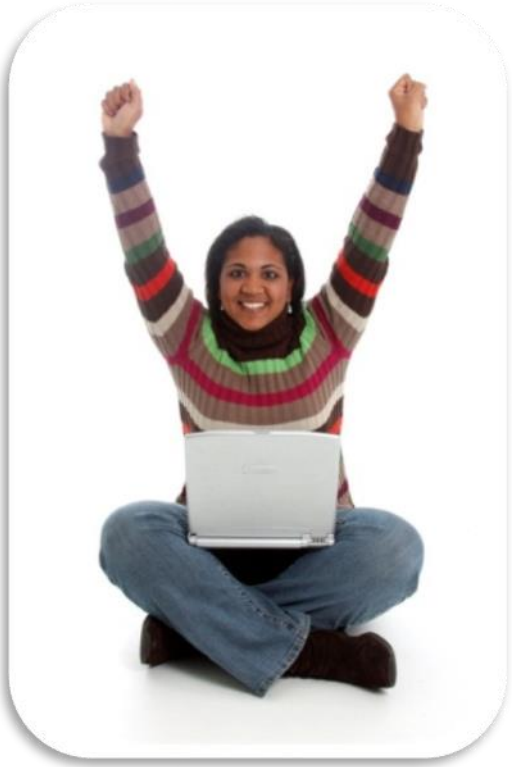
Social Media

Social Media

- What to do about workforce posting about/to patients?
- How to respond to patient communications through social media?
- How are smartphone cameras used?
- What is organization's social media presence?
- Do you have a social media policy?

Social Media Action Items

- Sensitize/train workforce
  - Social media (and the Internet) is forever
  - “Private” is not private
  - How to respond to friend requests – It is OK to say no in the work environment
  - Social media can and does have consequences
  - What you say on social media reflects on you and the organization



Social Media

- Train on permissible/impermissible use of social media
  - "I hate the patient I treated today" is not allowed
  - "I hate my boss" is fine
- Consequences of posting patient information/photos
- Clarify who may speak for the organization
- Authorizations when patient information/images are posted

Documentation

Document, Document, Document: Security

- Adage: If it wasn't documented, then it wasn't done
- Does your documentation demonstrate all your HIPAA compliance efforts?
- Risk analysis
  - Revisiting risk analysis
- Risk management
  - Evidence that corrective actions has been taken
  - Completed weekly checklists that security tasks (e.g., audit log review) have been completed
  - Screenshots of relevant configurations (e.g., encryption on server is enabled)
  - Minutes of security matters being presented to board
- Designation of Security Official

Document, Document, Document: Privacy

- Appropriate uses and disclosures
- Individual rights
  - Response to requests
  - Notice of Privacy Practices
- Policies and procedures
- Training
- Designation of Privacy Official
- Sanctions

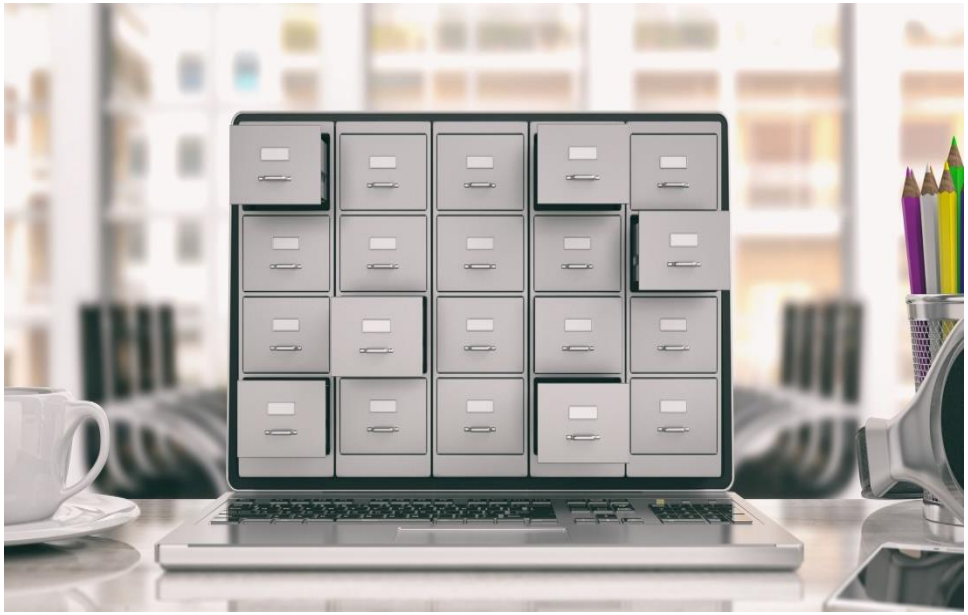
Document, Document, Document: Breach Notification

- Burden of Proof on Covered Entity/Business Associate
- Case Study (True Story): An encrypted laptop is stolen. A terminated IT employee files a complaint with OCR claiming that you failed to report a breach
- Can you produce documentation:
  - Evidencing when all laptops were encrypted?
  - Demonstrating that the stolen laptop was encrypted?
  - The user could not turn off encryption on the laptop?
  - That affected employees were trained?
  - Notifications were/were not made appropriately?
  - Actions were taken “without unreasonable delay”

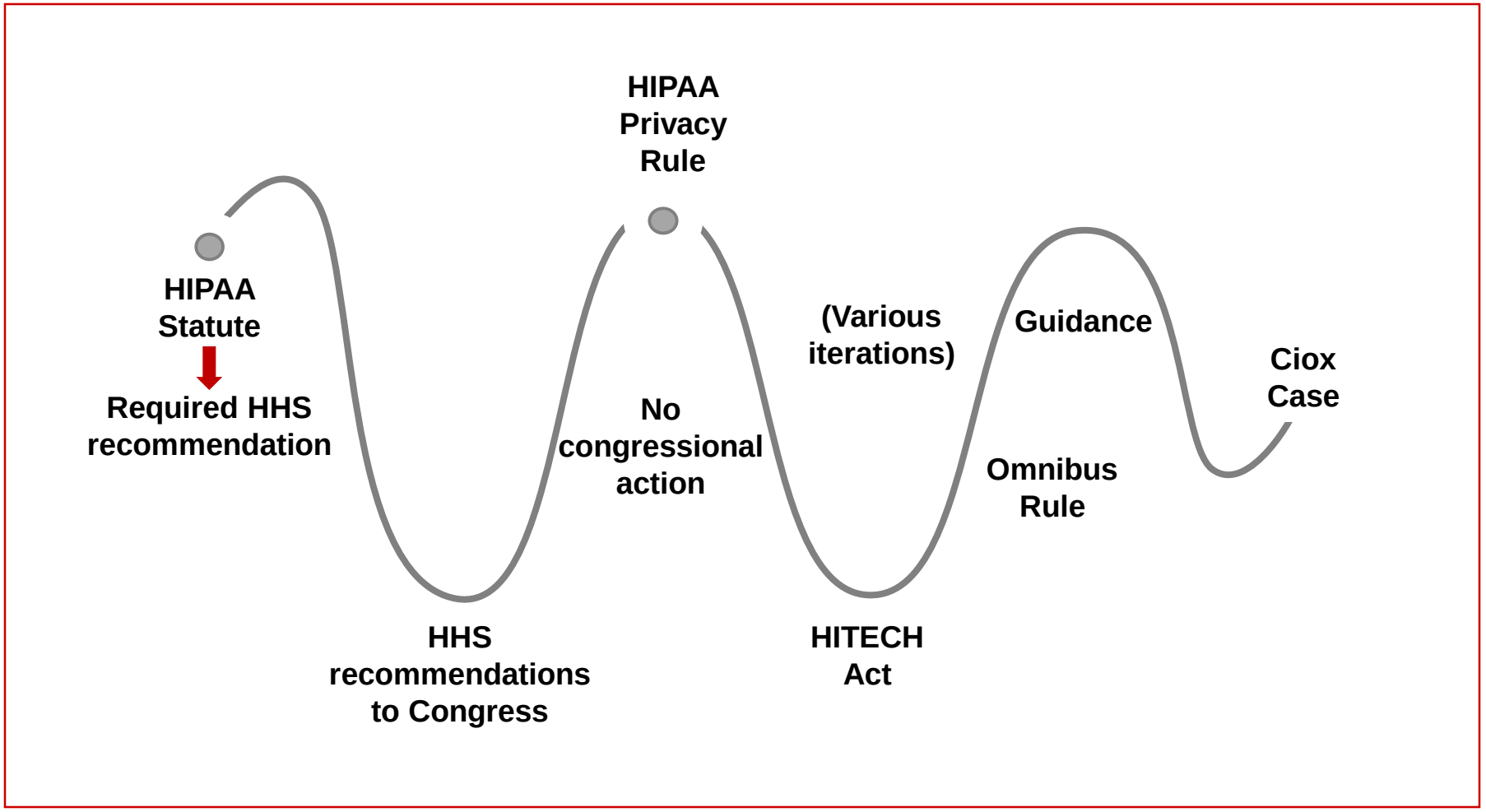
Access to PHI

Access to PHI

- HIPAA grants individuals a right of access to PHI
- High priority for OCR
- But the rules have changed



Access – But First a Story



Access to PHI: Ciox Case

- Ciox Healthcare, LLC
  - Release of Information vendor
- Fees
- Claimed HHS's interpretation
  - Expanded the pool of disclosures subject to the lower "Patient Rate"
  - Cost ROI vendors millions of dollars a year
- Brought suit to challenge HHS

Access – Third Party Directive

- Initial Privacy Rule: Individuals may request copies of/access to PHI in a designated record set (subject to certain exceptions)
- HITECH: Permits Individuals to direct Covered Entities to forward electronic copies of PHI in an EHR to third parties
- Omnibus Rule: Extended the access right of Individuals to direct all PHI (regardless of media) to third parties

- Ciox Court: Invalidated Omnibus expansion
  - 3P directive only for electronic copies of PHI from EHR

Access – “Patient Rate”

- Covered Entities may charge only a “reasonable, cost-based fee” so cost will not impede Individuals’ access
  - Yes: Costs of copying, postage
  - No: Data storage, document retrieval
- HITECH – Extended “Patient Rate” to electronic PHI from EHR
- Guidance – Clarified Patient Rate extends to all Individual requests (no matter the recipient)
- Court – Patient Rate only for Individual requests going to Individual

Questions