Morgan Lewis

How to Prepare for a HIPAA Audit

Privacy Check ✓

www.morganlewis.com

Presenters:
Sage Fattahian
Lauren Licastro
Georgina O'Hara

April 17, 2012

Historical Perspective

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- April 2003: Privacy Rule is effective
  - Sets standards to limit how Protected Health Information (PHI) is used and disclosed, and to provide individuals with certain rights related to their PHI
- April 2005: Security Rule is effective
  - Defines administrative, physical, and technical safeguards necessary to protect confidentiality, integrity, and availability of electronic PHI (ePHI)

Historical Perspective

- American Recovery and Reinvestment Act of 2009
  - Includes the Health Information Technology for Economic and Clinical Health Act (HITECH)
- February 2010: HITECH becomes effective
  - Amends Privacy Rule and Security Rule; adds Notification of Breach provisions; strengthens enforcement and increases penalties for violations
- Spring/summer 2012: Omnibus Regulations

Penalties

- Significant civil and criminal penalties may be imposed
  - Civil penalties: As high as $1.5 million for multiple violations of the same requirement in a calendar year
  - Criminal penalties: As high as $250,000 and 10 years of imprisonment
  - Enforcement:
    - *Civil enforcement by HHS/OCR*
    - *Criminal actions prosecuted by DOJ*
    - *State Attorneys General*

Current Enforcement Activity

- Periodic audits
  - Pilot program to audit 150 covered entities by end of 2012
    - *Notice and document request*
    - *On-site visit*
    - *Report*
    - *Follow-up investigation if serious compliance issues revealed*
- Investigation of breach reports
  - HHS will follow up on significant breaches

Assess Your Compliance

- Regularly perform a “Self-Audit”
  - Recommendation: Every 2 years
  - Track the flow of PHI through the entire organization
  - Involve all key people
  - Use an audit questionnaire or a similar tool as a guide

Assess Your Compliance

- Review all documentation for consistency with practices and legal accuracy
  - *Policies and Procedures*
  - *Notice of Privacy Practices*
  - *Authorization*
  - *Plan Sponsor Certification/Plan Language*
  - *Business Associate Agreements*

Train Your Workforce

- Training, training, training
  - Recommendation:
    - *Within 60 days of hire*
    - *Refresher every 2 years*
  - Focus on legal requirements and practical application to job duties
    - *Use examples*
    - *Conduct quizzes*
  - Track and log participation

Danger Zones

- Individual rights
  - Procedure in place
  - Coordinate with Business Associates
  - Timely respond
- Complaints
  - Take all complaints seriously
  - Investigate thoroughly with the involvement of counsel
  - Respond adequately and timely

Danger Zones

- Breaches
  - Have notification procedure in place
    - *Business Associates*
  - Identify team to investigate
    - *Include Privacy Officer and counsel*
  - Properly document investigation and findings
  - Take action
    - *Mitigate harm*
    - *Prevent future breaches*

Examples of Violations

- Recent enforcement actions
  - Cignet Health of Maryland
    - *First time OCR imposed a civil money penalty under HIPAA*
    - *$4.3 million civil penalty*
      - $100 per day for failure to respond to patient requests
      - $1.5 million per year for failure to cooperate with OCR
  - Massachusetts General Hospital
    - *$1 million settlement*
    - *Corrective action includes new policies and procedures regarding transporting PHI; training*

Examples of Violations

- UCLA
  - *$865,500 settlement*
  - *Corrective action includes independent monitor*
- BlueCross BlueShield of Tennessee
  - *$1.5 million settlement*
  - *First reported settlement with health plan*
  - *Corrective action includes training new hires within 40 days*

- Other examples

Ways to Avoid Violations

- Do NOT delay in notifying Privacy Officer of *suspected* breach
- Have detailed policies and procedures – especially for breach-prone areas
  - Removal of hard copy PHI
  - Laptop use
  - Smartphones
  - Storage
- Train employees at all levels

Your Action Plan

- Regularly self-audit
  - Track PHI and ePHI and review documentation
  - Train workforce
  - Provide Privacy Officer with necessary resources and support to respond timely to:
    - *Requests for individual rights*
    - *Complaints*
    - *Breach investigations*
    - *HHS inquiries/audits*

Questions?

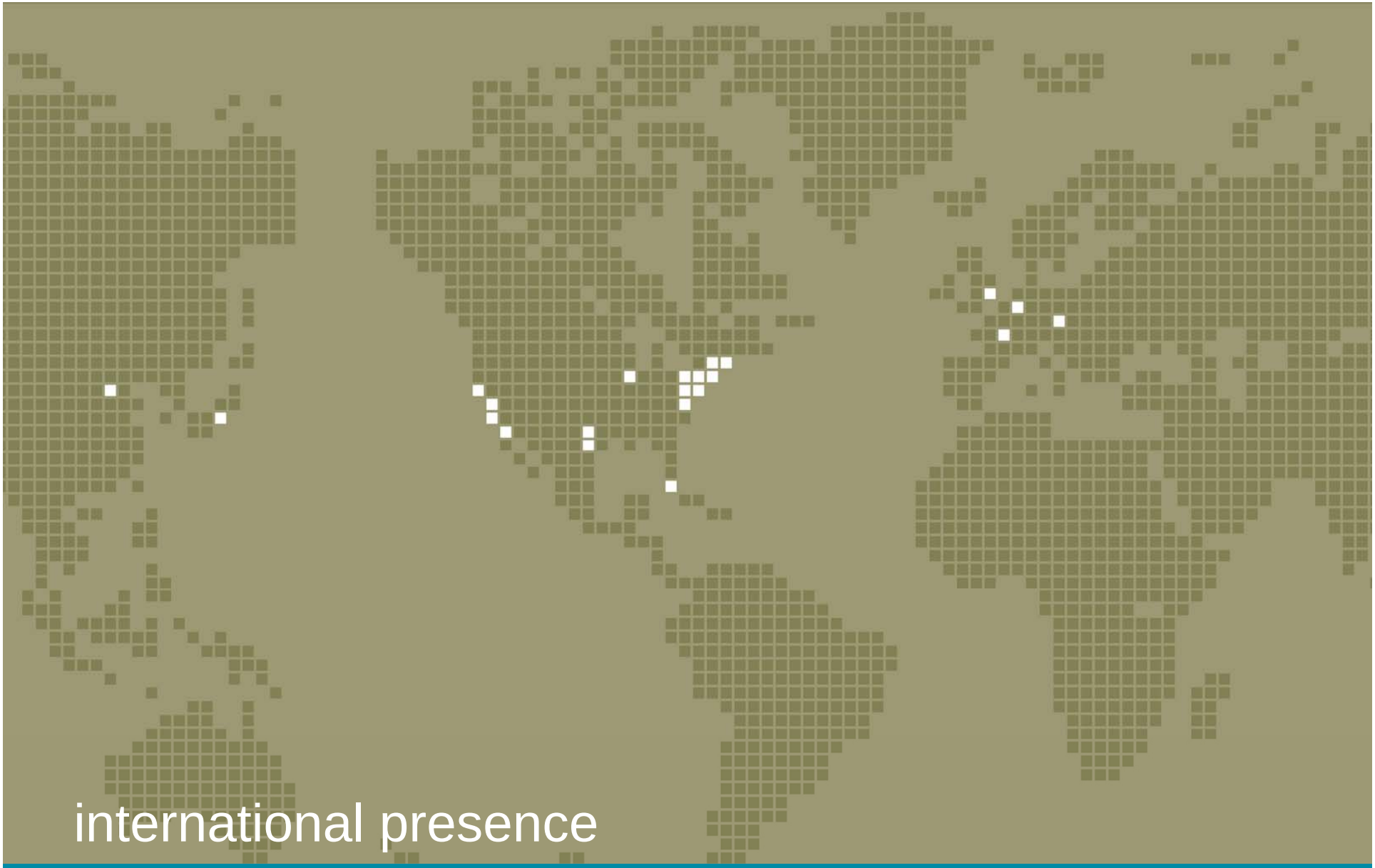
Presenters

- Lauren Licastro
  - 412.560.3383
    - *llicastro@morganlewis.com*
- Sage Fattahian
  - 312.324.1744
    - *sfattahian@morganlewis.com*
- Georgina O’Hara
  - 215.963.5188
    - *go'hara@morganlewis.com*

DISCLAIMER

- This communication is provided as a general informational service to clients and friends of Morgan, Lewis & Bockius LLP. It should not be construed as, and does not constitute, legal advice on any specific matter, nor does this message create an attorney-client relationship.

- **IRS Circular 230 Disclosure**
  To ensure compliance with requirements imposed by the IRS, we inform you that any U.S. federal tax advice contained in this communication (including any attachments) is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing, or recommending to another party any transaction or matter addressed herein. For information about why we are required to include this legend, please see http://www.morganlewis.com/circular230.



international presence

Beijing Boston Brussels Chicago Dallas Frankfurt Harrisburg Houston Irvine
London Los Angeles Miami New York Palo Alto Paris Philadelphia Pittsburgh
Princeton San Francisco Tokyo Washington Wilmington