Morgan Lewis

HIPAA Privacy Compliance Initiative: Final Rules Impact Employer Health Plans

Presenters:
Sage Fattahian
Lauren Licastro
Georgina O'Hara

Date: February 8, 2013
Time: 12:30-1:30 p.m. ET

Agenda

- History of HIPAA & HITECH
- Omnibus Regulations
  - Business Associates
  - Breach Notification
  - Notice of Privacy Practices
  - Enforcement
  - Other Changes
- Next Steps
- Questions?

History of HIPAA & HITECH Act

- Health Insurance Portability & Accountability Act of 1996 (HIPAA)
  - Privacy (effective 2003) & Security (effective 2005)
- Health Information Technology for Economic and Clinical Health (HITECH) Act – Effective February 2010
- Omnibus Regulations
  - Effective date: March 26, 2013
  - Compliance date: September 23, 2013 (w/ exception)
  - "Marks the most sweeping changes to the HIPAA Privacy & Security Rules since they were first implemented."

Omnibus Regulations

- Business Associates (BA)
  - Extends direct liability to BAs for Security & certain Privacy compliance
  - Expands definition of BA
    - *e.g., Subcontractor of BA*
    - *Additional guidance planned*
  - Affirms liability for acts of "agents"
  - Modifies content of BA Agreements (BAAs)
    - *Comply by September 23, 2013, or September 23, 2014 if …*
  - No additional time for BAs to comply

Omnibus Regulations

- Breach Notification
  - Eliminates subjective "significant risk of harm" threshold
  - Presumes breach requiring notification
    - *Unless CE/BA demonstrates "low probability that PHI [protected health information] has been compromised"*
    - *Consider at least 4 factors*
    - *Objective standard*
  - Likely to increase breach reporting
  - Additional guidance planned
  - Note: Methodology for counting violations remains unclear

Omnibus Regulations

- Other Changes
  - Genetic Information
    - *Prohibits plans from using or disclosing genetic info for underwriting purposes*
  - Marketing & Sale of PHI
    - *Only permitted with authorization*
  - Individual Rights
    - *Restrict disclosure to plan when paying out of pocket*
    - *Access to PHI in the form and format requested*

Omnibus Regulations

- Notice of Privacy Practices (NPP)
  - Revise for:
    - *Certain uses & disclosures requiring authorization*
    - *Fundraising*
    - *Breach Notice*
    - *GINA*
  - Redistribution
    - *Post by September 23, 2013 & provide in next annual mailing*

Omnibus Regulations

- Enforcement
  - Retains 4 tiers of penalties
    - *Did not know – $100 - $50,000*
    - *Due to reasonable cause – $1,000 - $50,000*
    - *Due to willful neglect & timely corrected – $10,000- $50,000*
    - *Due to willful neglect & not timely corrected – $50,000 - $1.5M*
  - Secretary of Labor required to investigate complaint or to conduct compliance review where willful neglect probable
  - Factors used in determining amount of civil money penalty

Next Steps

- Perform Gap Analysis/Self-Audit Now
- Revise Policies & Procedures
- Revise & Post/Distribute Notice of Privacy Practices
- Revise Business Associates/Subcontractor Agreements
  - Consider approach
- Train Privacy Employees
- Consider Encryption

How We Can Help?

- Morgan Lewis Benefits Solutions
  - HIPAA Privacy Initiative
    - *Self-Audit Assistance*
      - Includes detailed audit questionnaire
      - Identification of potential violations
    - *Training*
      - May be recorded for future use
    - *Privacy Officer Assistance*

Polling Question

- If you are interested in learning more about our HIPAA compliance services, please answer the polling question on the right-hand side of your screen and we will give you a call.

DISCLAIMER

- This material 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. These materials may be considered Attorney Advertising in some states. Please note that the prior results discussed in the material do not guarantee similar outcomes. Links provided from outside sources are subject to expiration or change.

- **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.

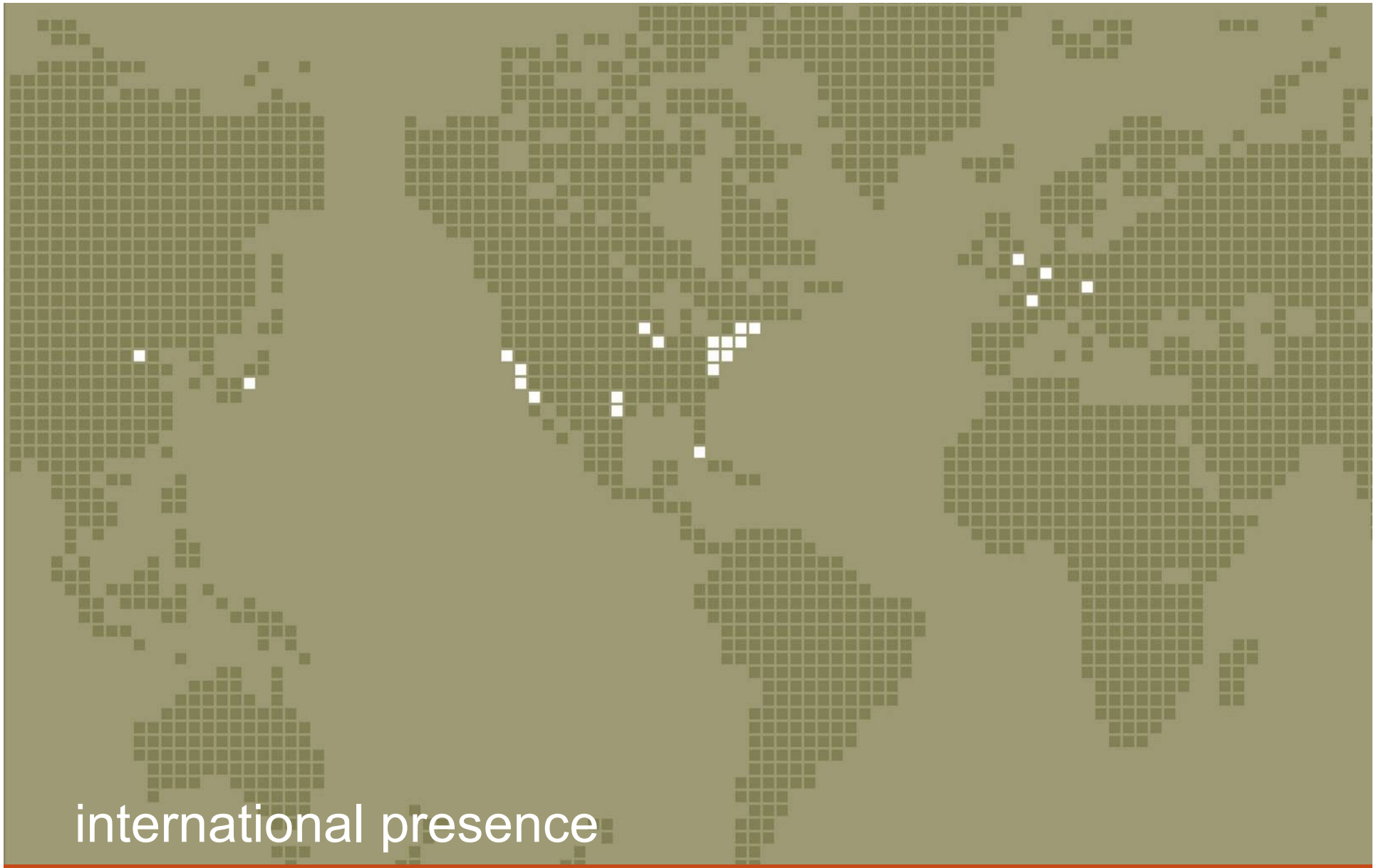
Contact Information

Lauren Licastro
Pittsburgh
412.560.3383
llicastro@morganlewis.com

Sage Fattahian
Chicago
312.324.1744
sfattahian@morganlewis.com

Georgina O'Hara
Philadelphia
215.963.5188
go'hara@morganlewis.com

Morgan Lewis



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