

HITECH ACT UPDATE **HIPAA BREACH NOTIFICATION RULE** **WEB CAST**

David G. Schoolcraft
Ogden Murphy Wallace, PLLC
dschoolcraft@omwlaw.com

Presenters

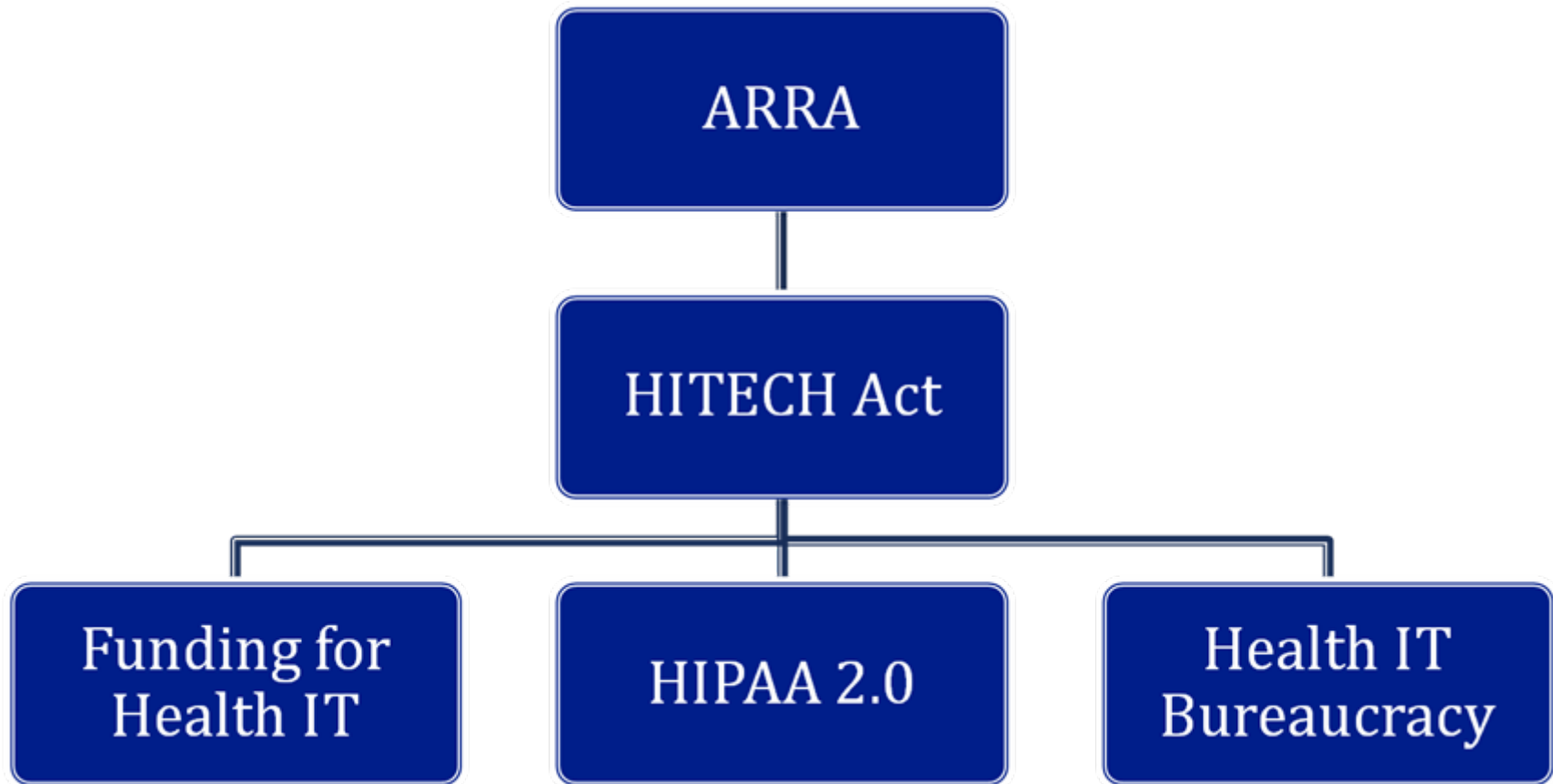
- ▶ David Schoolcraft,
Member, Ogden Murphy Wallace, PLLC



- ▶ Taya Briley,
General Legal Counsel, WSHA



HITECH Health Reform



OBJECTIVES

1. Review Breach Notification Rule
2. Incident Analysis Examples
3. Compliance Action Plan

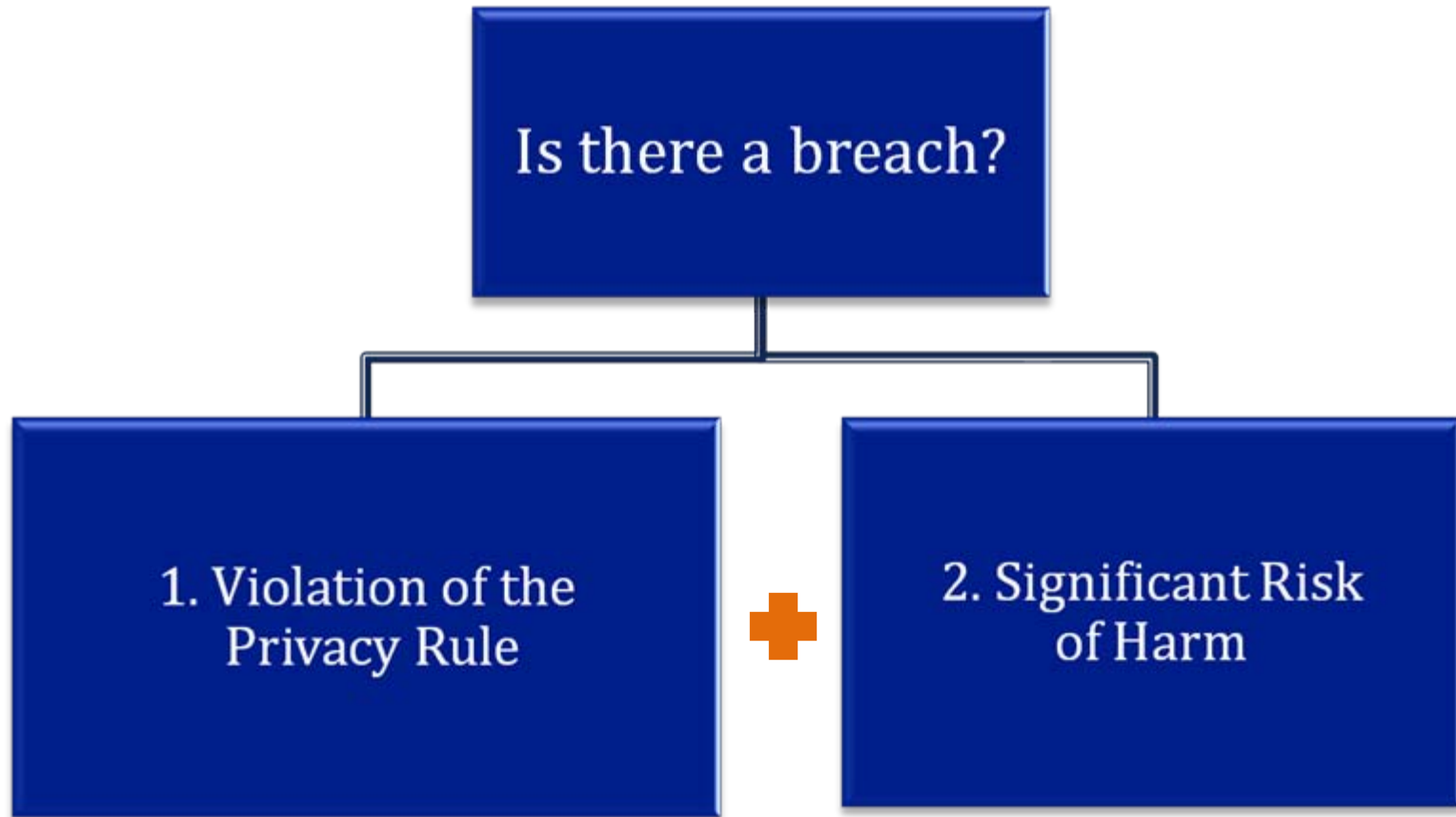
Effective Date: September 23, 2009

Breach Notification Rule

“A **covered entity** shall, following **discovery** of a **breach** of **unsecured protected health information**, **notify** each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been accessed, acquired, used, or disclosed as a result of such breach.”

- 45 CFR §164.404(a)(1)

A. Is There a Breach?



Significant Risk of Harm

- ▶ Harm Threshold
 - Incident must impose a “**significant risk of financial, reputational or other harm to the individual.**”
- ▶ Fact Specific Analysis
 - What is the nature of the information?
 - To whom was the information disclosed?
 - Mitigation efforts matter.

B. Was PHI “unsecured”?

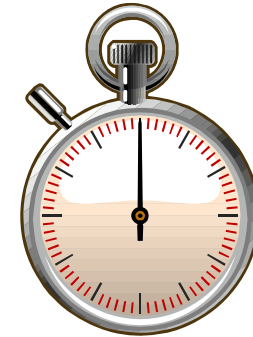
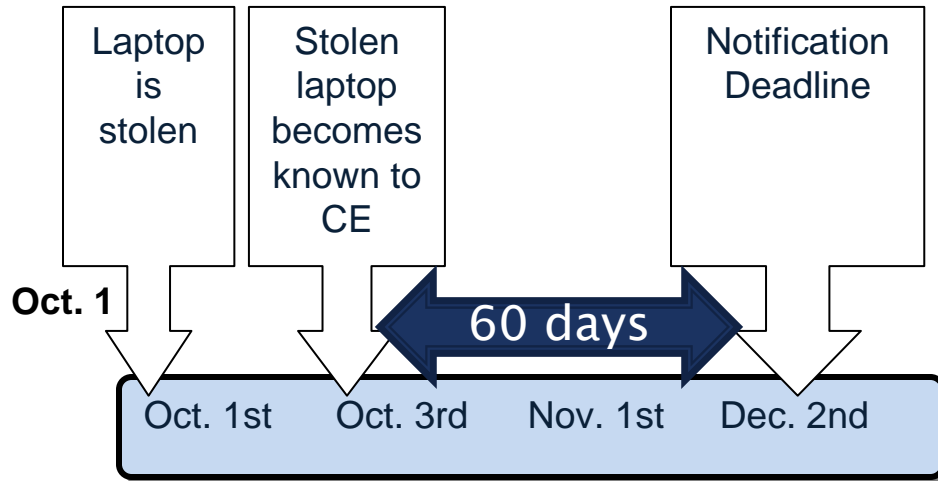
- ▶ Was data “unusable, unreadable, or indecipherable to unauthorized individuals”?
- ▶ Safe Harbor Standards:
 - National Institute of Standards and Technology (NIST) publications:
 - 800-111 (Encryption)
 - 800-52 (Transport Layer Security)
 - 800-77 and 800-113 (VPNs)
 - 800-88 (Guidelines for Media Sanitation)
 - NIST publications available at www.csrc.nist.gov

Incident Analysis Examples

- ▶ Stolen laptop--
 - What if data is encrypted?
 - What if laptop is password protected?
 - What if data limited to basic directory information?
 - What if laptop is recovered?
- ▶ Data sent to wrong recipient--
 - Other healthcare provider?
 - Employer?
- ▶ “Incidental disclosure”
- ▶ Technical security breach.

Timeliness of Notice

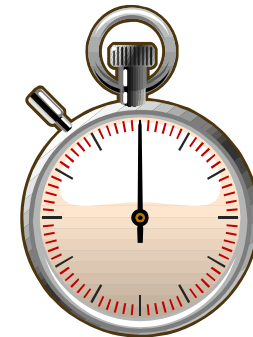
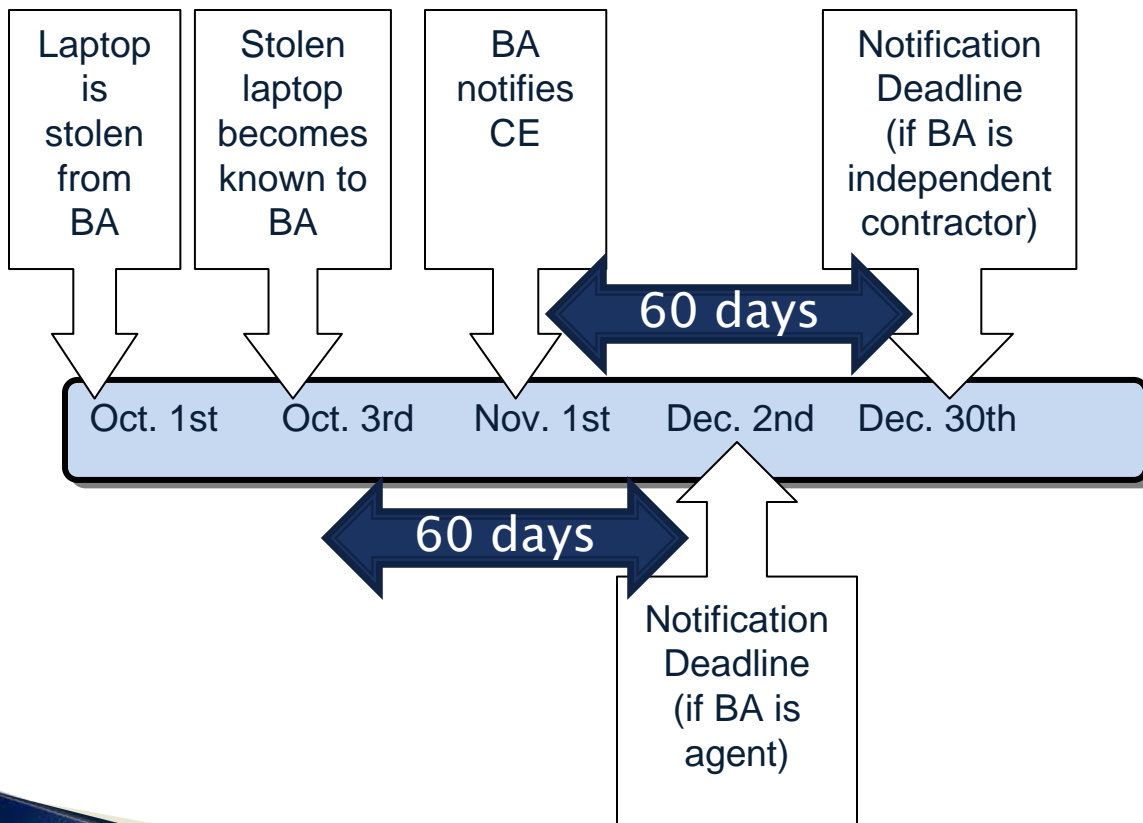
- ▶ 60 day shot-clock from date of *discovery*
- ▶ Without “**unreasonable delay**”



Failure to provide notification within 60 days may lead to violation

Timeliness of Notice

- ▶ What if a business associate is involved?



Failure to provide notification within 60 days may lead to violation

Content of Notice to Individuals

- ▶ Brief description of what happened
 - Date of breach
 - Date of discovery of breach
- ▶ Description of the types of PHI disclosed
- ▶ Steps individual should take to protect him/herself
- ▶ Description of what covered entity is doing to:
 - Investigate breach
 - Mitigate harm to individuals - i.e. provide fraud insurance, suggest that individual contact credit bureau or credit care company
 - Protect from further breaches
- ▶ Contact procedures--Toll free number, Website or postal address

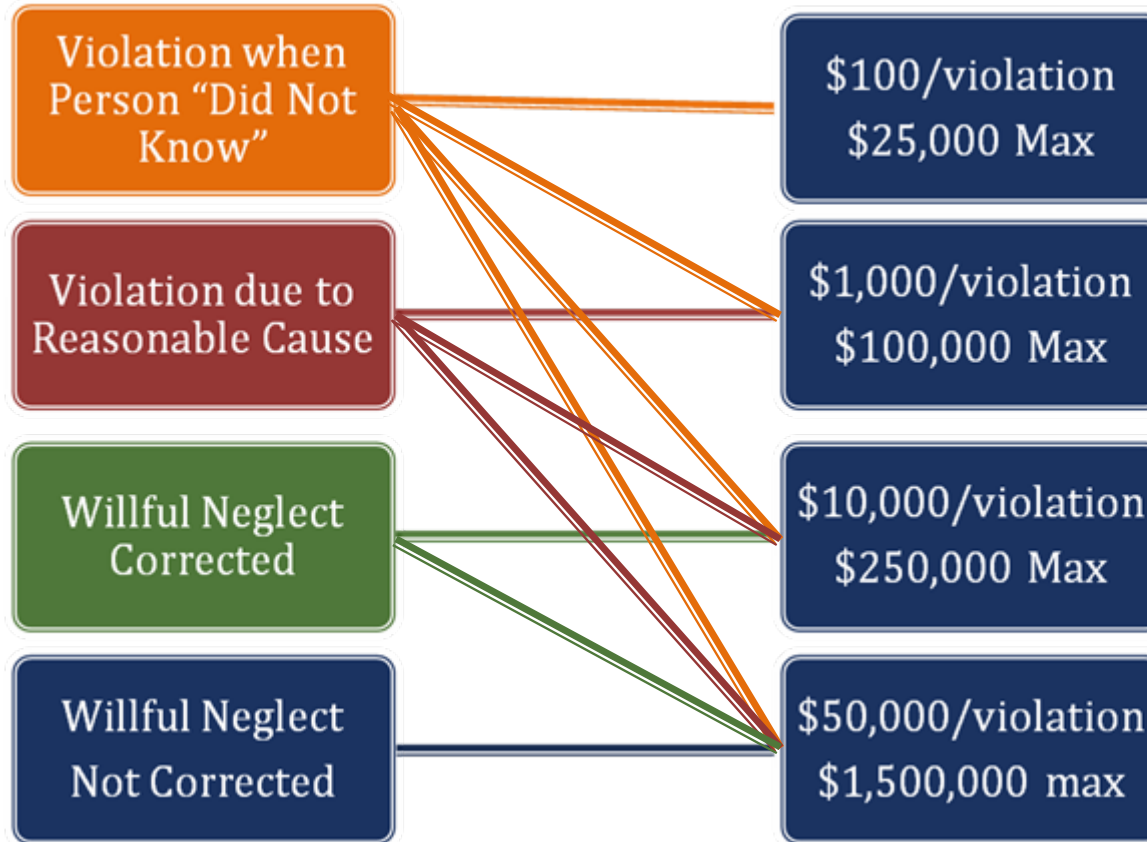
Additional Notice Recipients

- ▶ **Media Notice - Required if Over 500 Individuals**
 - Supplemental to written notice; must still provide individual notice
 - Prominent media outlets serving a State or jurisdiction
 - Contains the same content as written notice
- ▶ **Notice to HHS**
 - Over 500 individuals - notice required within 60 days
 - Less than 500 then CE maintains a log and reports all breaches within 60 days after calendar year using HHS form

Administrative Requirements

- ▶ Effective September 23, 2009
- ▶ Enforcement discretion to February 22, 2010
- ▶ Covered Entity has the burden of proof
 - Must maintain documentation evidencing that all notifications were made in accordance with these rules
 - If no notification then evidence as to why it was not necessary
- ▶ Training
- ▶ Implementation of Policies & Procedures
- ▶ Maintenance of breach log for end of year report to HHS

Increased Civil Penalties



HHS shall base the penalty determination on the nature & extent of the violation and the nature & extent of the resulting harm.

**Effective for all violations after Feb. 17, 2009
but not enforced until Feb. 17, 2010**

Compliance Action Plan

What CEs **Must** Do Now

- ▶ Develop policies & procedures.
 - Create a checklist of requirements in case of breach
- ▶ Train workforce members.
- ▶ Identify key individuals for incident analysis and response.

Compliance Action Plan

What CEs **Should** Do Now

- ▶ Analyze data posing high risk
 - Ex: Mobile Data
- ▶ Encryption if possible/practical
- ▶ Analyze Business Associate Agreements
 - Independent Contract vs. Agent
 - Requirements to notify covered entity if breach
- ▶ Review insurance policies

Compliance Action Plan

What to do if an **Incident Occurs**

- ▶ Perform incident analysis
 - Was there a “breach”?
 - Violation of HIPAA Privacy Rule?
 - Significant risk of harm?
 - Statutory exceptions?
 - Was data encrypted?
- ▶ If necessary, report breach under notification rule:
 - 60 day requirement.
 - Notice to individual.
 - Notice to media and HHS?

APPENDIX

Breach Definition Statutory Exceptions

- ▶ HITECH Act contains additional statutory exceptions to definition of “breach”.
 - Unintentional use or disclosure to workforce member if use or disclosure was made in good faith and did not result in further use or disclosure
 - Inadvertent disclosure from an individual authorized to access the records to another similarly situated individual
 - Unauthorized person could not have reasonably retained the information.
 - Limited data set excluding Date of Birth and Zip Codes

Questions?

David G. Schoolcraft
dschoolcraft@omwlaw.com

206.447.7211

Health Law Blog: www.omwhealthlaw.com