Business Associate Considerations for the HIE Under the Omnibus Final Rule

Joseph R. McClure, Esq.
Counsel
Siemens Medical Solutions USA, Inc.

WEDI Privacy & Security Work Group Co-Chair

Agenda

- Who is a Business Associate?
- Omnibus Final Rule Impacts to Business Associates
- Business Associate Agreements under HITECH
- Role of Governance of HIEs as Business Associates

Who is a Business Associate??

- Final Rule: An entity that "…***creates, receives, maintains, or transmits [PHI] for a function or activity regulated by [HIPAA]…***" on behalf of a Covered Entity
- Final Rule expanded the definition of Business Associates to include:
  - **Health Information Organizations** (HIEs and RHIOs)
  - E-prescribing Gateways
  - PHR providers on behalf of a CE
  - Patient Safety Organizations
  - **Subcontractors** that create, receive, maintain, or transmit PHI on behalf of BAs
- **Subcontractor** means a person whom a BA delegates a function, activity, or service, other than in the capacity of a member of the workforce of such BA
- Mere Conduit vs. Business Associate with Routine Access to PHI

Summary of Impacts to Business Associates Under HITECH Omnibus Final Rule

- The Final Rule requires BAs to comply with the HIPAA Security Rule in the same manner as a CE
- Disclosure of PHI must be kept to limited data set or minimum necessary
- BA must comply with the certain HITECH Privacy requirements to the extent applicable to BA's services and access to PHI on behalf of CE
  - Health Provider must honor a request by an individual to restrict disclosure of PHI to a Health Plan if the individual pays for associated service out-of-pocket in full
  - Individual has right to a copy of PHI in an electronic format
  - Sale of PHI prohibited unless authorized by individual
  - Certain marketing communications require authorizations
- Let's not forget Breach Notification Obligations
- BAs subject to direct enforcement by HHS Office for Civil Rights

Business Associate Agreements

- Final Rule clarified the required additional HITECH BAA provisions:
  - BA required to comply with Security Rule obligations
  - BA must report to CE any breach of unsecured PHI as required by the Breach Notification Rule
  - BA must enter into BAAs with subcontractors imposing the same obligations that apply to BA
  - BA must comply with the Privacy Rule to the extent the BA is carrying out a CE's obligations under the Privacy Rule
- Other Considerations
  - Agency Relationship – a CE (or BA) is liable for the acts or omissions of its downstream entity acting within the scope of "agency"
  - Implementation Time-Line - Up to one additional year – 9/22/2014
  - Data Security Agreements

HIE Governance for Nationwide Health Information Exchange

- ONC's Documented Framework for HIE Governance
  - Increase interoperability
  - Increase trust among participants of the HIE
  - Decrease cost and complexity
- Organizational Principles – identify general approaches for good self governance
- Trust Principles – Guide entities on patient privacy, data access and data management
- Business Principles – financial and operational policies and transparency
- Technical Principles – use of standards to support Trust and Business principles as well as promoting interoperability

- Resource: http://www.healthit.gov/policy-researchers-implementers/health-information-exchange-governance

Joseph R. McClure, Esq.
Counsel
Siemens Medical Solutions USA, Inc.

joseph.mcclure@siemens.com

610-219-9101