SIEMENS

Practical Steps to Implementing ARRA for Business Associates

Joseph R. McClure, Esq.
Regulatory & Compliance Principal, HDX Operations
Siemens Medical Solutions USA, Inc.
Revenue Cycle Solutions

SIEMENS

About Siemens and HDX

- Siemens is a global company with strong US presence in various areas, including electronics, industry, energy, infrastructure, and healthcare.
- Siemens Medical Solutions USA, Inc. is a major provider of integrated healthcare IT solutions, bringing together imaging and lab diagnostics, therapy and healthcare IT.
- Healthcare Data Exchange (HDX) was started in 1989 and is the EDI Clearinghouse within the Healthcare IT Division of Siemens Medical Solutions.
- HDX's secure value-added EDI transaction services support every aspect of the healthcare revenue cycle workflow via integrated and web-based solutions.
- Today HDX provides a range of EDI services to approximately 1,500 of the largest healthcare delivery, acute care, and ambulatory care organizations nationwide.
- HDX connects healthcare providers with over 340 of the nation's top payers.
- HDX processed more than 280 Million EDI transactions in 2009.

Agenda

- Key Business Associate Provisions in HITECH
- Who is a Business Associate?
- Business Associate Agreements and Contracting
- Implementing HIPAA Security and Privacy
- Questions

Key Business Associate Provisions in HITECH

- Direct Enforcement of HIPAA Security Rules to Business Associates (§ 13401)
  - Enforceable against Business Associates the same as Covered Entities
  - Requires Implementing Administrative, Physical & Technical Safeguards
  - Risk Assessment Needed
  - Encryption of Data
  - Monitor HHS for new Guidance, Rules & Regulations
- HITECH Privacy Provisions Applicable to Business Associates (§ 13404)
  - Enforceable against Business Associates the same as Covered Entities
  - Breach Notification
  - Accounting of Disclosures
  - Restrictions on Certain Disclosures
  - Restrictions on Sale of PHI or Use for Certain Marketing Activities

Key Business Associate Provisions in HITECH

- Enhanced Enforcement – Civil & Criminal Penalties
  - Possible civil penalties even for unintentional acts; greater potential penalties for violations due to willful neglect and/or failure to correct
  - Penalties range from minimum of $100 per violation up to max of $1.5 Million in a calendar year
  - Individuals who report violators to be given a share of the penalties imposed
  - Potential liability at both the entity level and individual workforce level
  - OCR to implement audit program
  - Enforcement by State Attorneys General

Who is a Business Associate Anyway??

- Evaluate Your Own Identity as a Business Associate
  - Identify the parties with whom you do business – both up & down stream
  - What do you do for them? What do they do for you?
  - Is PHI involved in any way? If so, how?
- Business Associates Have been Further Identified/Defined in HITECH (§ 13408)
  - Business Associate Agreement **Required** if an entity:
    - Provides data transmission services involving PHI
    - To a Covered Entity **OR** its Business Associates
    - That requires routine access to such PHI
  - E.g., HIEs, RHIOs, ePrescribing Gateway Vendors and PHR Vendors that provide a PHR as part of a service offered to individuals by a Covered Entity

Business Associate Agreements and Contracting

- Do you currently have Business Associate Agreements (BAAs) in place?
- Create Comprehensive List of all Contracted Entities and assess whether BAA agreement is already executed. If not, is a BAA needed?
- Prepare to Engage Your Business Partners in the BAA Process
  - Review your standard BAA against new HITECH Requirements
  - Engage Legal Counsel to draft any needed HITECH Updates to your BAA
  - Most entities seem to have their own standard BAA, but it is always good to have your own version so you know where your organization stands on certain issues and where to start from a negotiation position

Business Associate Agreements and Contracting

- HITECH has Something to Say About Business Associate Agreements:
  - "[HIPAA security and HITECH privacy requirements] shall be incorporated into the business associate agreement between the business associate and the covered entity." HITECH §§ 13401(a), 13404(a).
- Does "shall be incorporated" mean:
  - New provisions are incorporated by law without further action by the parties?
  - Parties are directed to amend/execute BAAs to include the new provisions?
- Parties should plan to amend/execute BAAs with new provisions, but new Business Associate rules may further dictate when, how, or even if this is *required* by law

Business Associate Agreements and Contracting

- Common HITECH Provisions to Include in BAAs (if applicable)
  - Acknowledgement that business associate is subject to direct enforcement of HIPAA Security and HITECH Privacy provisions
  - Agreement that business associate will implement the HIPAA Security Rule for safeguarding PHI – Administrative, Physical & Technical Safeguards
  - Encryption of PHI on portable devices and removable media
  - Breach Notification – timing of notice, form of notice, evaluation of harm
  - Minimum Necessary Use and Disclosure of PHI – use of limited data set
  - Restrictions on Certain Disclosures
  - Marketing and Fund Raising
  - Accounting of Disclosures – made through an electronic health record
  - Individual Right of Access to an Electronic Copy of PHI
  - Prohibition on the Sale of PHI

Implementing HIPAA Security and Privacy

- Prepare to Evaluate/Implement HIPAA Security Safeguards
  - Designate an Individual to be Responsible for Review and Implementation
  - NIST Special Publication (SP) 800-66 is a good starting point; provides helpful guidance on implementing HIPAA Security
- Security Risk Assessment (SRA) Required under HIPAA
  - Even if you have already completed a SRA, HIPAA requires this be revisited as part of an ongoing Risk Management Program
  - The SRA will help you identify areas of vulnerability against safeguards you may already have in place, and should also identify areas where you may need to implement additional safeguards
  - NIST SP 800-30 is a good place to start
  - Several other NIST publications available for evaluating and managing risk

- All NIST Publications available at: http://csrc.nist.gov/publications/PubsSPs.html

Implementing HIPAA Security and Privacy

- Documented Policies and Procedures – Review, Implement and/or Update, e.g.:
  - Employee Screening and Annual Privacy and Security Training
  - Document Retention
  - Role-based Access to Confidential Data
  - Strong Passwords and Password Security Management
  - Physical Security
  - Monitoring Compliance – sanctions for violations of policy
- Review/Update Data Encryption Policies
  - Data at Rest – NIST SP 800-111
  - Data in Motion – NIST SPs 800-52, 800-77, 800-113
  - Data Destruction – NIST SP 800-88
- Monitor for new Regs/Guidance from HHS and be ready to update policies

- All NIST Publications available at: http://csrc.nist.gov/publications/PubsSPs.html

Implementing HIPAA Security and Privacy

- If Appropriate, Consider Industry Accreditations as a Means of:
  - Assessing,
  - Implementing, and
  - Demonstrating Compliance
  - with HITECH & HIPAA Privacy and Security
- E.g., Electronic Healthcare Network Accreditation Commission (EHNAC) http://www.ehnac.org – has accreditation programs for:
  - Healthcare Networks (EDI Vendors, Payers, etc.)
  - Health Information Exchanges
  - ePrescribing
  - Financial Services (Banks, etc.)
  - Outsourced Services (Vendors that support EHNAC-accredited entities)
  - Application Service Providers of Electronic Health Records

Questions??

Joseph R. McClure, Esq.
Regulatory & Compliance Principal, HDX Operations
Siemens Medical Solutions USA, Inc.
Revenue Cycle Solutions

joseph.mcclure@siemens.com

610-219-9101