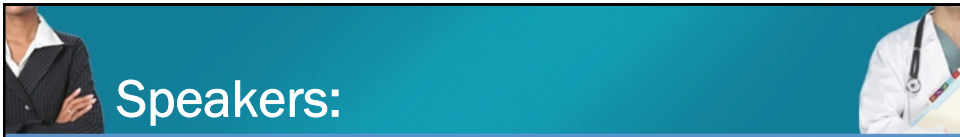


HEALTH INFORMATION TECHNOLOGY
WEB CONFERENCE SERIES


**Key Legal Issues Raised by Electronic Health
Records Technology**
Friday, November 18, 2011

FOLEY
FOLEY & LARDNER LLP


©2011 Foley & Lardner LLP • Attorney Advertising • Prior results do not guarantee a similar outcome • Models used are not clients but may be representative of clients • 321 N. Clark Street, Suite 2800, Chicago, IL 60654 • 312.832.4500 4837-7158-9389.1 11.8158




Speakers:




Chanley Howell
Partner
Foley & Lardner LLP




Jim Kalyvas
Partner
Foley & Lardner LLP
Chair of Information
Technology &
Outsourcing Practice



Dan Orenstein
Senior Vice President,
General Counsel and
Secretary of the Board
Athenahealth, Inc.



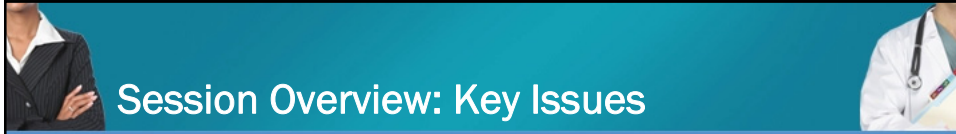
Rick Rifembark
Senior Counsel
Foley & Lardner LLP



Mike Scarano
Partner
Foley & Lardner LLP
Vice Chair of Health
Care Industry Team

©2011 Foley & Lardner LLP

2
11.8158

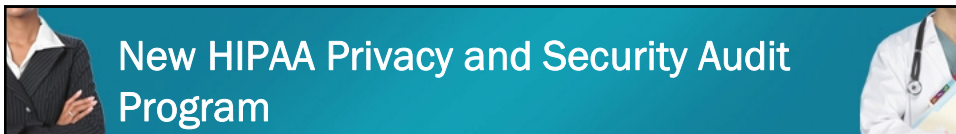


Session Overview: Key Issues

- HIPAA privacy and security audits
- EHR “meaningful use” incentive payments
- EHR subsidy programs
- Cloud computing
- Expansion of EHR regulation

©2011 Foley & Lardner LLP 3

11.01.08



New HIPAA Privacy and Security Audit Program

- Mandated by the HITECH Act
- OCR Intends to perform up to 150 audits between now and the end of December 2012 as part of a pilot program
 - A broad cross section of covered entities will be targeted
 - Business associates will be included after the initial phase

©2011 Foley & Lardner LLP 4

11.01.08



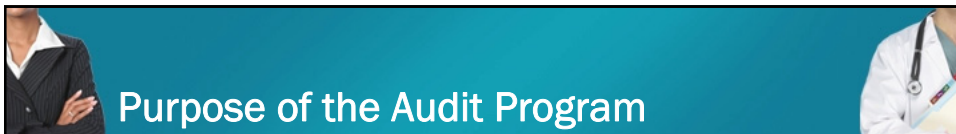
New Audit Program

- Protocols developed by KPMG as part of a \$9 million engagement to develop and implement the program
- Standard auditing protocol to be used
 - Letter will be sent requesting policies, procedures and other materials
 - Site visit will include interviews of key personnel
 - Draft report will be shared with the entity for comment and corrective action

©2011 Foley & Lardner LLP

5

11.01.08





Purpose of the Audit Program

- “Audits are primarily a compliance improvement activity”
- Should an audit reveal serious non-compliance, OCR will initiate a compliance review
- OCR will not post a listing of audited entities or the findings that would identify them

©2011 Foley & Lardner LLP

6

11.01.08





Medicare and Medicaid EHR Incentive Programs

- The American Recovery and Reinvestment Act of 2009 allocates billions of dollars in incentive payments to encourage the adoption of EHR
- Hospitals and “eligible professionals” qualify for incentive payments if they make “meaningful use” of “certified EHR technology”
- Medicare reimbursement adjustment if EHR “meaningful use” is not satisfied by 2015
- Hospitals may participate in Medicare and Medicaid EHR program; EPs must choose one

©2011 Foley & Lardner LLP 7

11.01.08




There are 3 Basic Requirements to Achieve Meaningful Use

- Meaningful use of “certified EHR technology”
 - Meaningful use means meeting the objectives and measures (for EPs, the 15 core and 10 menu set objectives and related measures)
 - Attestation to achievement of measures in 2011, with respect to a period of at least 90 days
- The use of certified EHR technology for electronic exchange of health information to improve quality of care
- Requirement to submit data on clinical quality measures to CMS

©2011 Foley & Lardner LLP 8

11.01.08



Definition of Certified EHR Technology

“Certified EHR Technology”

Complete EHR or combination of EHR modules:

- Meeting requirements of Qualified EHR **and**
- Tested and certified under the ONC certification program as having met all applicable certification requirements specified in 45 CFR Part 170

“Qualified EHR”

Electronic record of health-related information on an individual that includes patient demographic and clinical health information, such as medical history and problem lists, with capacity to do all the following:

- provide clinical decision support
- support physician order entry
- capture and query quality information
- exchange electronic health information with, and integrate such information from, other sources


“Complete EHR”:

EHR technology meeting *all* applicable HHS certification criteria

“EHR Module”:

Any service, component, or combination thereof that can meet requirements of at least one HHS certification criterion

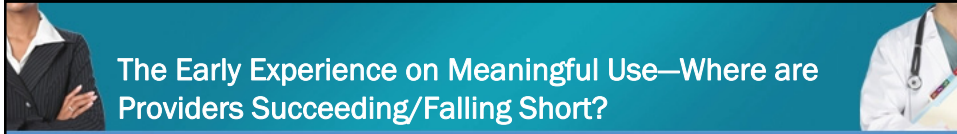
©2011 Foley & Lardner LLP 9



What are Vendors Offering in Terms of “Warranties” or “Guarantees” for Attaining Meaningful Use?

- Vendor offers can be plotted in a very broad range—check the fine print, for example:
 - Currently qualifies as certified EHR technology
 - Will always qualify as certified EHR technology
 - Will assist you, when used properly, to obtain meaningful use incentive payments
 - Specific guarantees/payments if it does not meet the criteria for certified EHR technology
 - Specific guarantees/payments if meaningful use incentive payments are not obtained


©2011 Foley & Lardner LLP 10



The Early Experience on Meaningful Use—Where are Providers Succeeding/Falling Short?

- According to data collected from athenahealth’s client base, physician practices have been challenged with the following meaningful use measures:
 - Provide clinical summaries
 - Measure: Providers must provide clinical summaries to patients for at least 50% of all office visits within three business days of the office visit.
 - This requires a high level of participation to achieve compliance, or alternatively, automated systems that ensure provision of the clinical summary.
 - Record demographic information
 - Measure: Providers must record preferred language, gender, race, ethnicity, and date of birth as structured data for at least 50% of all unique patients seen during the 90-day reporting period.
 - Some practitioners and staff have been reluctant to gather information on race, ethnicity.
 - Record vital signs
 - Measure: Providers must record height, weight, and blood pressure as structured data for more than 50% of all unique patients age 2 and over. The EHR must calculate and display body mass index (BMI) and plot and display growth charts.
 - Providers do not necessarily record vital signs at every office visit, for example if the patient has come in for multiple visits. Some specialists do not typically record vital signs.
 - Protect electronic health information
 - Measure: Perform a security risk assessment and implement mitigating steps.
 - This measure is left to clients so is difficult to measure, but polls indicate spotty compliance

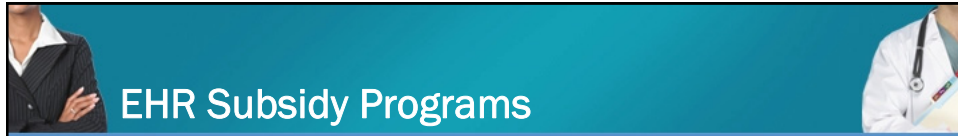
©2011 Foley & Lardner LLP 11
11.8158



EHR “Meaningful Use” Incentive Payments: Other Practical Issues

- Exclusion of hospital-based EPs
- Medicare v. Medicaid EHR incentive program for EPs
- Reassignment of EHR incentive payments by employed or contracted EPs
- Maintaining documentation to support “meaningful use” attestation

©2011 Foley & Lardner LLP 12
11.8158



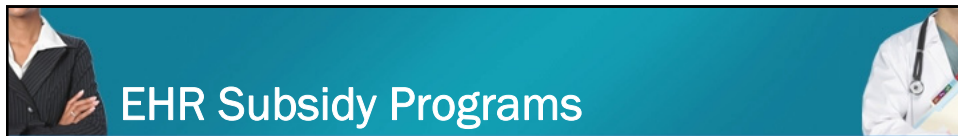
EHR Subsidy Programs

- Rationale/Origins
 - Stark Law and Anti-Kickback Statute (AKS) limit certain financial relationships with physicians
 - August 2006: AKS EHR safe harbor and Stark Law EHR exception promulgated
 - Intended to facilitate the adoption EHRs to improve quality of care, patient safety, and health care efficiency, while also maintaining security and privacy

©2011 Foley & Lardner LLP

13

11.01.08



EHR Subsidy Programs

- What EHR technology may be subsidized?
 - Donated items and services must be used predominately to create, maintain, transmit, or receive EHR. Examples include:
 - Rights, licenses and IP related to EHR software,
 - Interface and translation software,
 - Connectivity services (including wireless internet),
 - Clinical support and information services related to patient care,
 - Maintenance services, help desk, and similar support

©2011 Foley & Lardner LLP

14

11.01.08

A teal header banner with a businesswoman on the left and a doctor on the right. The text "EHR Subsidy Programs" is centered in white.

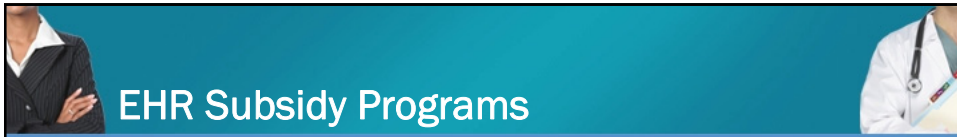
EHR Subsidy Programs

- What EHR technology may be subsidized?
 - EHR software may have ancillary functions, provided that the EHR functions predominate and that the ancillary functions directly relate to the care and treatment of individual patients
 - Donors cannot provide:
 - Hardware,
 - Staff (e.g., staff to transfer paper records to electronic format),
 - Software with core functionality other than EHR,
 - Monetary remuneration

©2011 Foley & Lardner LLP

15

11.01.08

A teal header banner with a businesswoman on the left and a doctor on the right. The text "EHR Subsidy Programs" is centered in white.

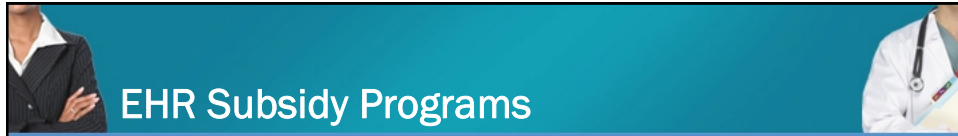
EHR Subsidy Programs

- Key Stark/AKS Requirements:
 - The EHR software is interoperable at the time it is provided to the physician (and donor cannot limit or restrict the use, compatibility, or interoperability of the items or services with other EHR)
 - Before receipt of the items and services, the physician pays **15 percent** of the donor's cost for the items and services
 - Physician eligibility for EHR subsidy is not determined in a manner that **directly** takes into account the volume or value of referrals or other business generated between the parties

©2011 Foley & Lardner LLP

16

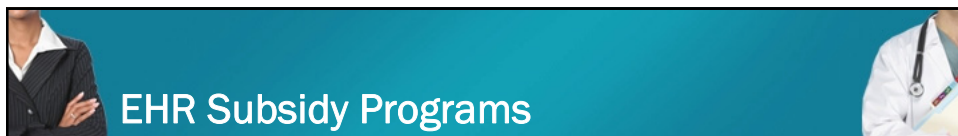
11.01.08



EHR Subsidy Programs

- Key Stark/AKS Requirements (cont.)
 - Written agreement between the parties sets forth the costs and other terms of the arrangement.
 - Signed by the parties;
 - Specifies the items and services being provided, the donor's cost of the items and services, and the amount of the physician's contribution; and
 - Covers all of the EHR items and services to be provided by the donor

©2011 Foley & Lardner LLP 17



EHR Subsidy Programs

- Key Stark/AKS Requirements (cont.)
 - The donor does not have actual knowledge of, and does not act in reckless disregard or deliberate ignorance of, the fact that the physician possesses or has obtained items or services equivalent to those provided
 - The items and services do not include staffing of physician offices and are not used primarily to conduct personal business or business unrelated to the physician's medical practice

©2011 Foley & Lardner LLP 18

EHR Subsidy Programs

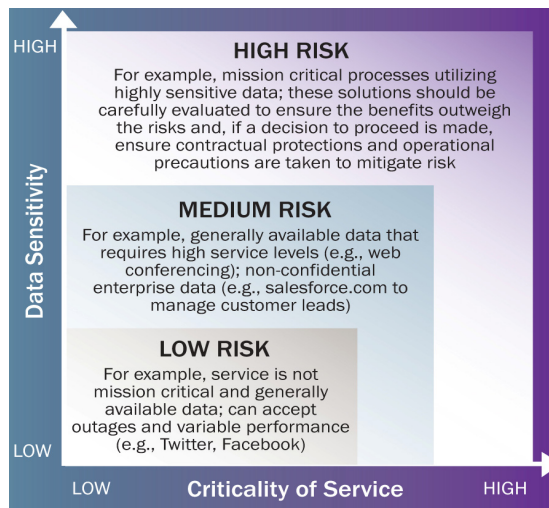
- Stark/AKS Requirements (cont.)
 - The transfer of the EHR items or services occurs and all conditions are satisfied on or before **December 31, 2013**
- Other Considerations
 - State laws
 - Patient privacy laws
 - IRS guidance
 - ACOs

©2011 Foley & Lardner LLP

19

11.01.08

Cloud Risk Assessment Matrix



©2011 Foley & Lardner LLP

20

11.01.08



NIST Cloud Road Map

- International Voluntary Consensus-Based Interoperability, Portability & Security Standards
- Solutions for High-Priority Security Requirements
- **Technical Specifications for High-Quality Service-Level Agreements**
- **Clear & Consistently Categorized Cloud Services**
- Frameworks to Support Federated Community Clouds

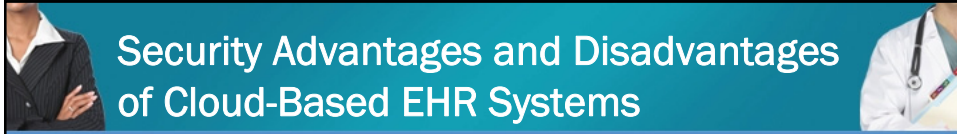
©2011 Foley & Lardner LLP 21
11.81.58



NIST Cloud Road Map

- Technical Security Solutions De-coupled from Organization Policy
- Defined Unique Government Requirements and Solutions
- Collaborative Parallel – Future Cloud Development Initiatives
- Defined & Implemented Reliability Design Goals
- **Defined & Implemented Cloud Service Metrics**

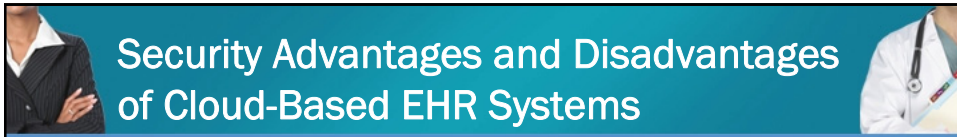
©2011 Foley & Lardner LLP 22
11.81.58



Security Advantages and Disadvantages of Cloud-Based EHR Systems

- **Disadvantages or Concerns About Cloud EHR**
 - What is “Cloud Computing”? According to NIST, Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction
 - Promise is greater flexibility and availability at a lower cost.
 - There are some concerns that require special attention when evaluating a cloud-based EHR system from a security standpoint
 - A number of these concerns are highlighted by the National Institute for Standards and Technology (“NIST”) in its “Guidelines on Security and Privacy in Public Cloud Computing,” January 2011, (available at http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf)

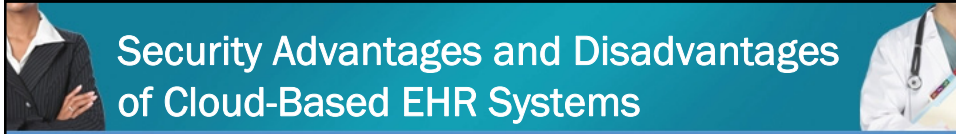
©2011 Foley & Lardner LLP 23



Security Advantages and Disadvantages of Cloud-Based EHR Systems

- **Cloud Security Concerns include:**
 - Nature of the Data: In health care, it often involves storage, access to, and transmission of, Protected Health Information (PHI)
 - System Complexity: Cloud computing environments can be more complex than traditional data centers. Can have a larger “attack surface.” Can include multiple services interacting together
 - Shared Multi-Tenant Environment: The “neighbors” can bring security risks. “Logical separation” among the tenants is required to provide adequate segregation of risk
 - Internet-Facing Services: Delivery over the Internet exposes clients to Internet infrastructure-related threats. Also potentially expands the attack surface
 - Loss of Control: Some security oversight is inherently delegated to a third party

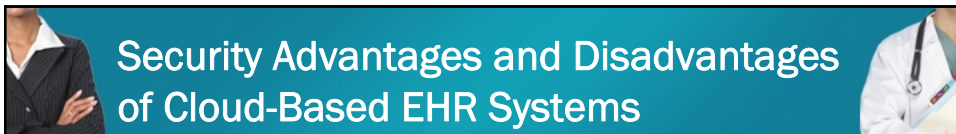
©2011 Foley & Lardner LLP 24



Security Advantages and Disadvantages of Cloud-Based EHR Systems

- **Cloud Security Advantages include:**
 - Staff Specialization: There are limited security resources in the industry. Vendors have the capability of employing a highly specialized security organization
 - Platform Strength: More uniform computing platform structure, which can facilitate better management of security protocols such as configuration control, vulnerability testing, security audits, patches. Strong, security-protective standards apply to certain entities, such as HIPAA, Payment Card Industries (PCI) standards, SAS-70 (SSAE-16), Sarbanes-Oxley
 - Availability - This is the often-ignored “third leg” of the security stool, for which the cloud offers big advantages. Built-in redundancy and disaster recovery at large scale can enhance this advantage

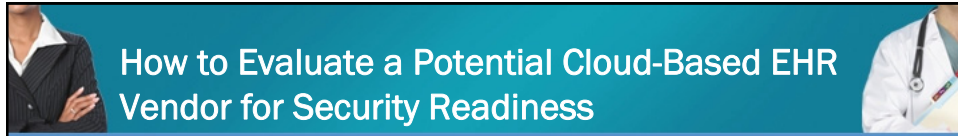
©2011 Foley & Lardner LLP 25
11.01.08



Security Advantages and Disadvantages of Cloud-Based EHR Systems

- **Cloud Security Advantages include:**
 - Back up and Recovery - Diverse geographies are available. Offsite backup is more readily supported
 - Data Concentration - Having the data in one place can be an advantage with a distributed workforce, because there is more assurance of data integrity when data is centralized
 - Mobile Endpoints - A cloud based architecture makes it easier to support mobile or thin client devices across a broad network. This can include pushing security patches to mobile devices

©2011 Foley & Lardner LLP 26
11.01.08



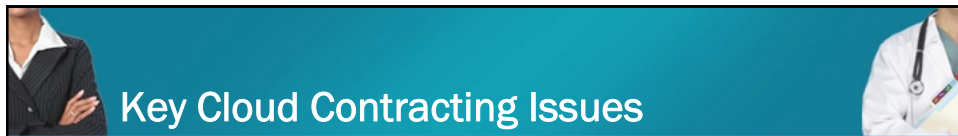
How to Evaluate a Potential Cloud-Based EHR Vendor for Security Readiness

- **Conduct your diligence**
 - At the end of the day, security diligence of a cloud-based vendor is essentially the same as the diligence you would conduct on a standard EHR vendor. The same security requirements apply (including the HIPAA security Rule)
 - Ask questions such as whether the vendor has conducted a HIPAA Security Risk Assessment
 - Ask if the vendor has a statement of security measures it would be willing to share with you
 - If you have specific concerns, ask to speak to the vendor's Chief Information Security Officer, or other individual with responsibility over security
 - Ask about the vendor's disaster recovery and business continuity programs. Understand the recovery time, and recovery points, as well as how comprehensive the program is

©2011 Foley & Lardner LLP

27

11.8158



Key Cloud Contracting Issues

- Due Diligence
- Availability / Service Levels
- Data Security
- Disaster Recovery / Business Continuity
- Data Ownership
- Data Conversion
- Insurance
- Indemnification

©2011 Foley & Lardner LLP

28

11.8158

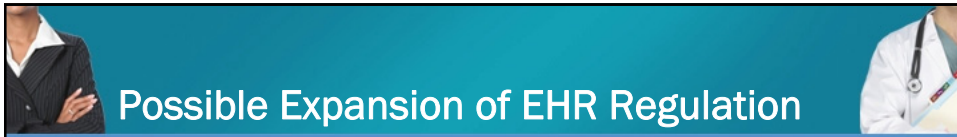


Key Cloud Contractual Issues

- Intellectual Property
- Limitation of Liability
- Implementation
- Fees
- Term
- Warranties
- Audit Rights

©2011 Foley & Lardner LLP 29

11.8158




Possible Expansion of EHR Regulation

- Institute of Medicine (IOM) Report on Patient Safety, November 8, 2011:
 - A "coherent structure" must be created to support provider and vendor reporting of adverse events related to EHR use. Affirmed by ONC.
 - Mechanism to report Health-IT related adverse events recommended.
 - Establish an independent federal entity to investigate Health-IT related incidents.
- Possibility of Food and Drug Administration (FDA) regulation
 - Regulation of EHRs as medical devices under a *pre-market approval* approach is raised from time to time
 - Medical Device Data Systems (MDDS) final regulation, February, 2011 – Integration of medical devices with EHRs could in some cases result in some regulation of the EHR as a Class I medical device. Requires registration and design controls (e.g., software development requirements)
 - EHR exemption – The FDA has stated numerous times that EHRs are subject to an exemption to medical device regulation, however the MDDS regulation creates some ambiguity
- Self-Regulatory Efforts (e.g., iHealth Alliance, voluntary reporting)

©2011 Foley & Lardner LLP 30

11.8158




Question & Answer Session

©2011 Foley & Lardner LLP

31

11.01.10



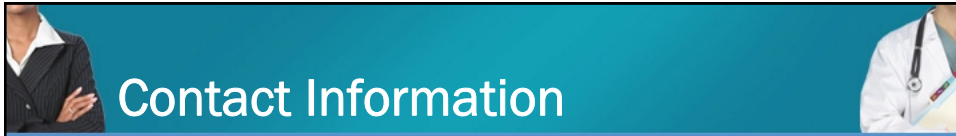
Mark Your Calendars

- There are two more sessions remaining as part of the **Health Information Technology Web Conference Series**:
 - Friday, December 16, 2011 - **Privacy and Security in the HITECH Era**
 - Monday, January 23, 2012 - **Emerging Issues in Health Information Technology**

©2011 Foley & Lardner LLP

32

11.01.10



Contact Information

- Chanley Howell – chowell@foley.com
- Jim Kalyvas – jkalyvas@foley.com
- Dan Orenstein – dorenstein@athenahealth.com
- Rick Rifembark – rrifembark@foley.com
- Mike Scarano – mscarano@foley.com