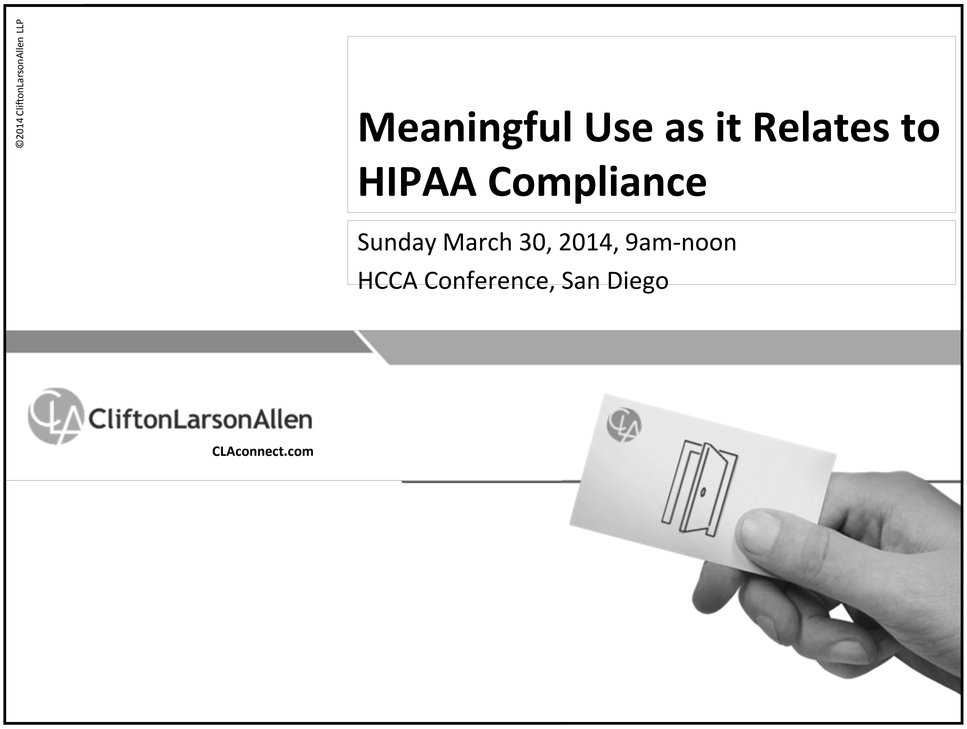
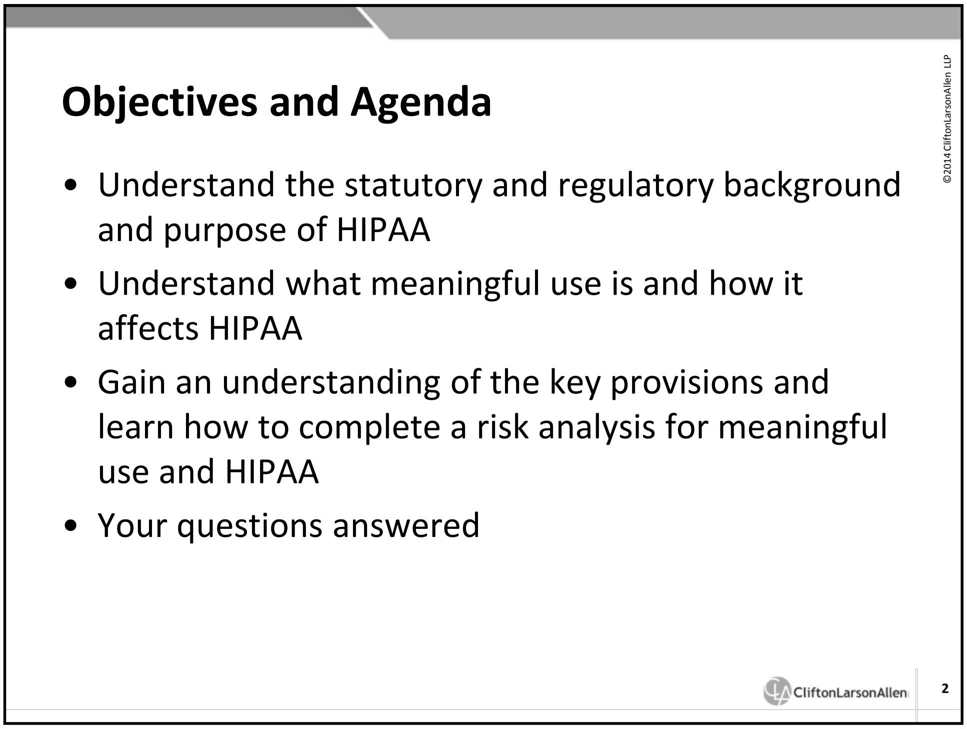


Meaningful Use as it Relates to HIPAA Compliance

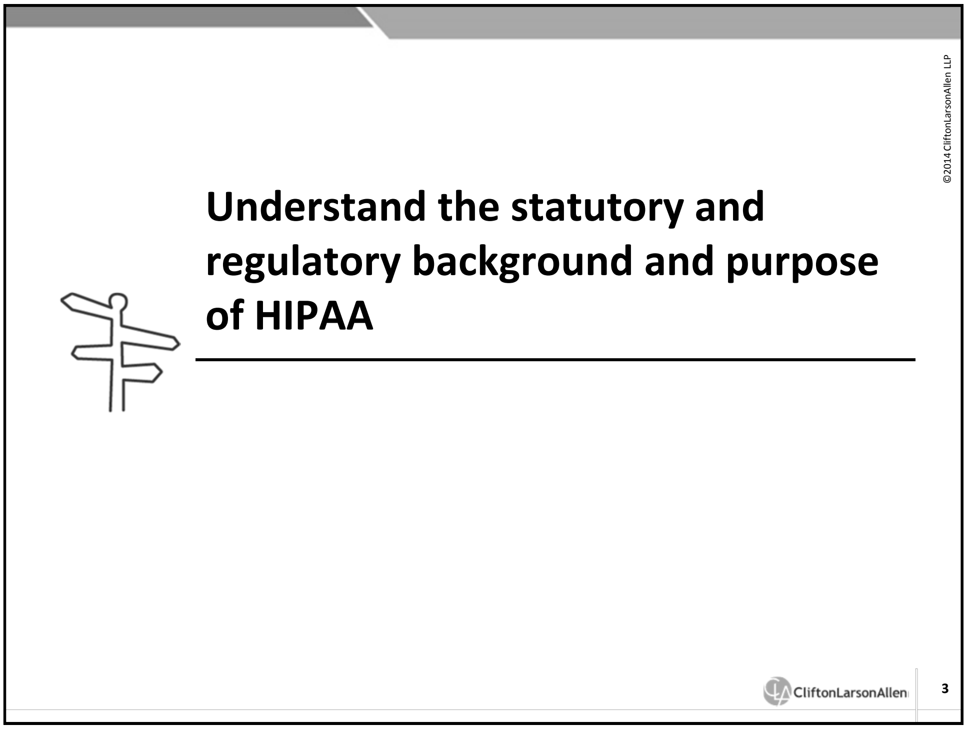
Sunday March 30, 2014, 9am-noon
HCCA Conference, San Diego

CliftonLarsonAllen
CLAconnect.com

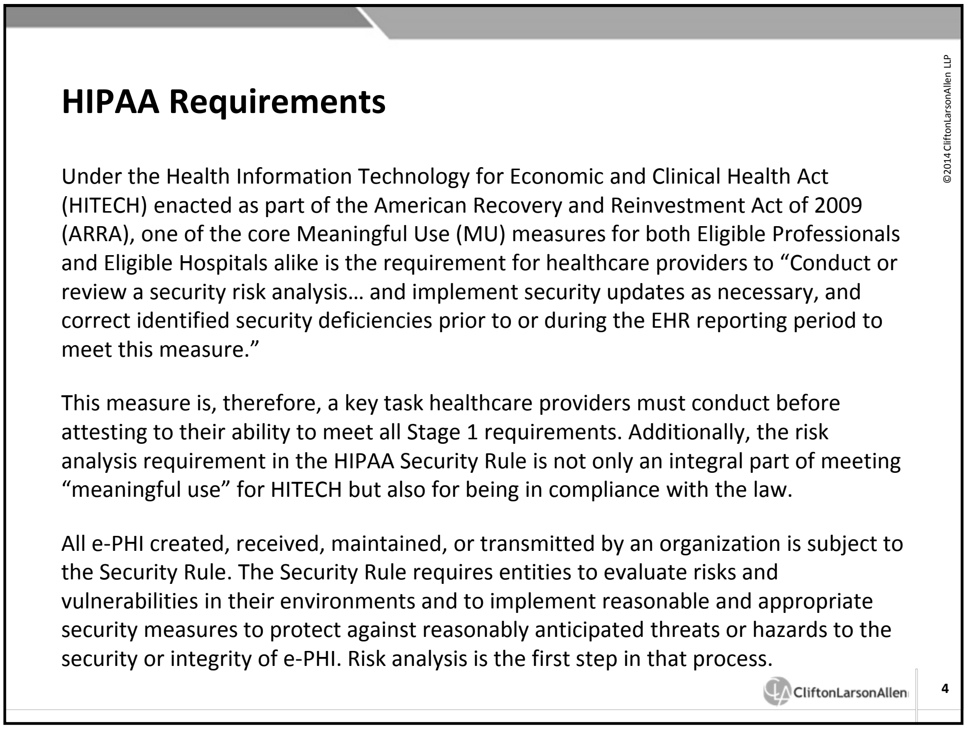


Objectives and Agenda

- Understand the statutory and regulatory background and purpose of HIPAA
- Understand what meaningful use is and how it affects HIPAA
- Gain an understanding of the key provisions and learn how to complete a risk analysis for meaningful use and HIPAA
- Your questions answered



Understand the statutory and regulatory background and purpose of HIPAA

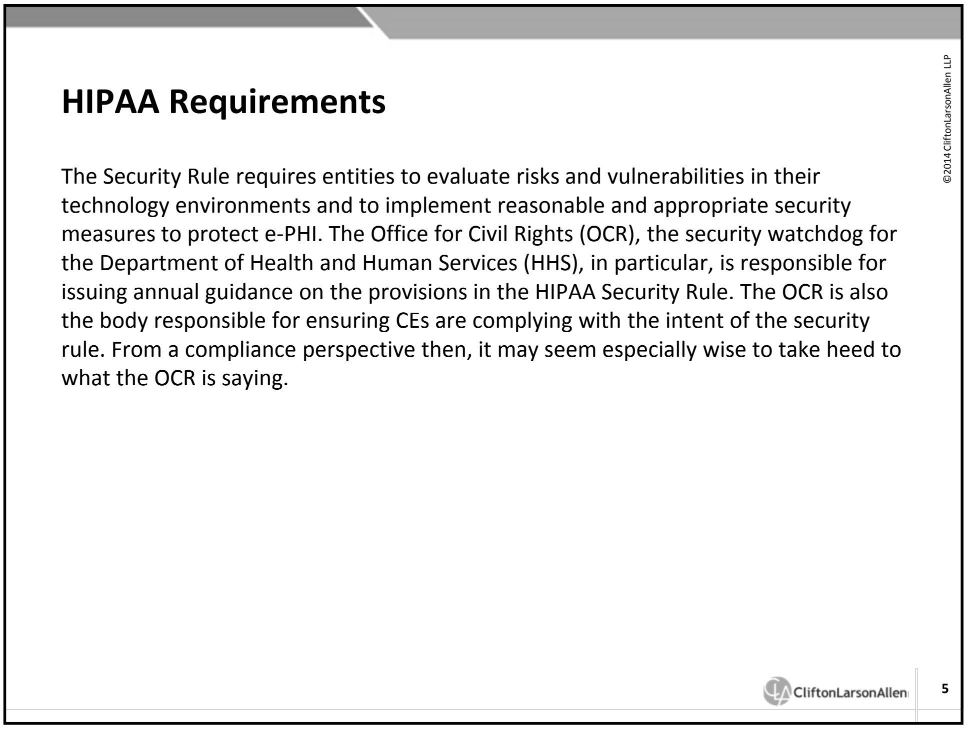


HIPAA Requirements

Under the Health Information Technology for Economic and Clinical Health Act (HITECH) enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA), one of the core Meaningful Use (MU) measures for both Eligible Professionals and Eligible Hospitals alike is the requirement for healthcare providers to “Conduct or review a security risk analysis… and implement security updates as necessary, and correct identified security deficiencies prior to or during the EHR reporting period to meet this measure.”

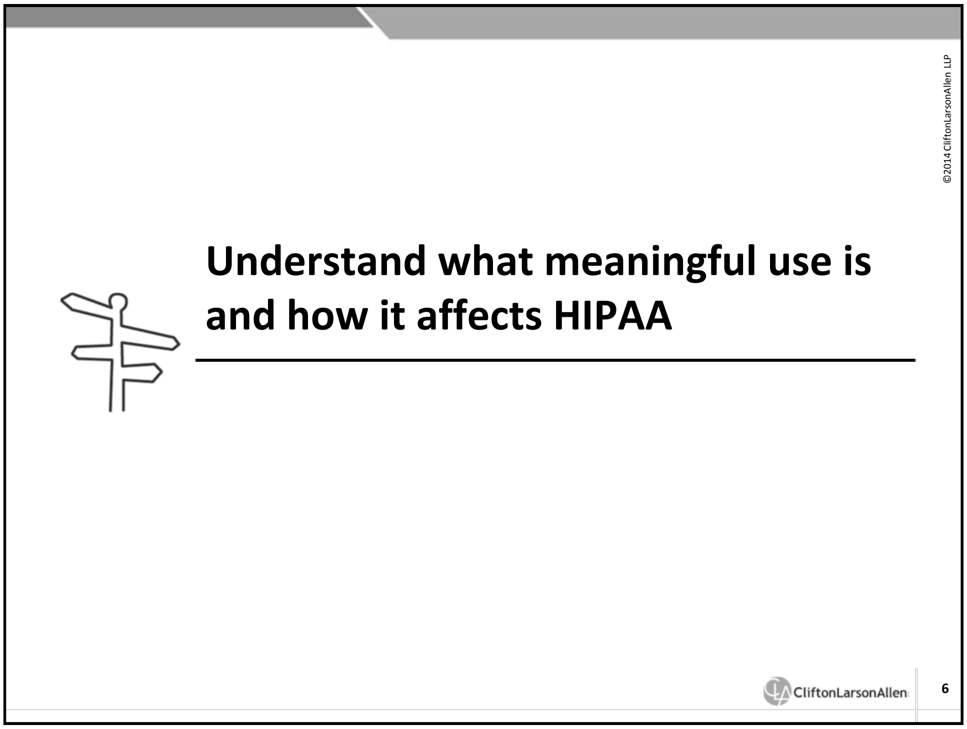
This measure is, therefore, a key task healthcare providers must conduct before attesting to their ability to meet all Stage 1 requirements. Additionally, the risk analysis requirement in the HIPAA Security Rule is not only an integral part of meeting “meaningful use” for HITECH but also for being in compliance with the law.

All e-PHI created, received, maintained, or transmitted by an organization is subject to the Security Rule. The Security Rule requires entities to evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of e-PHI. Risk analysis is the first step in that process.

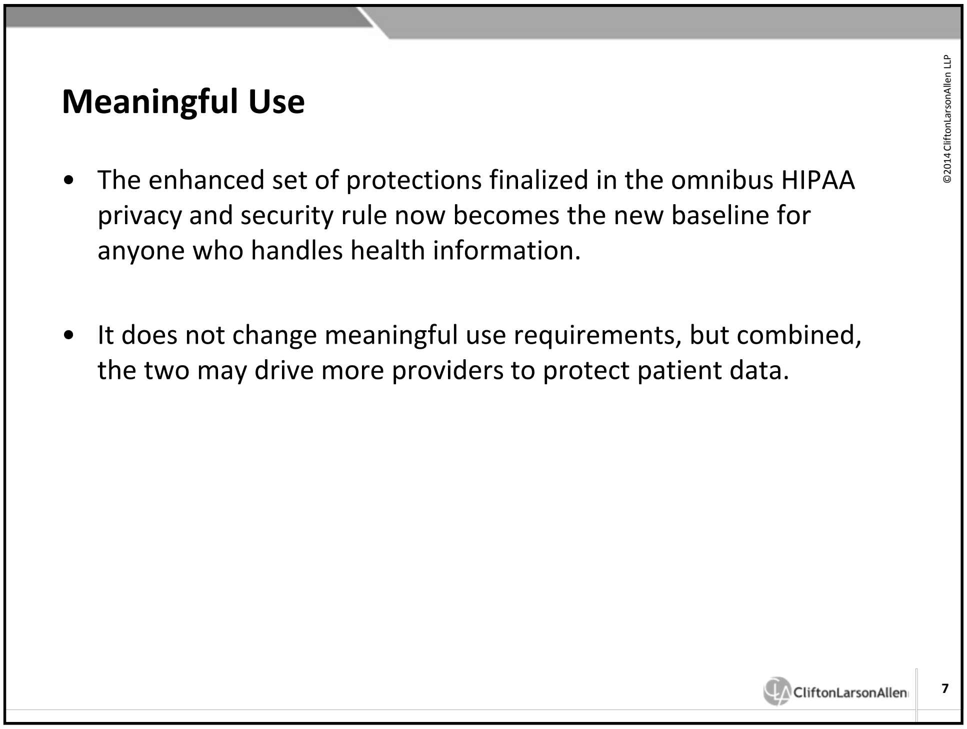


HIPAA Requirements

The Security Rule requires entities to evaluate risks and vulnerabilities in their technology environments and to implement reasonable and appropriate security measures to protect e-PHI. The Office for Civil Rights (OCR), the security watchdog for the Department of Health and Human Services (HHS), in particular, is responsible for issuing annual guidance on the provisions in the HIPAA Security Rule. The OCR is also the body responsible for ensuring CEs are complying with the intent of the security rule. From a compliance perspective then, it may seem especially wise to take heed to what the OCR is saying.

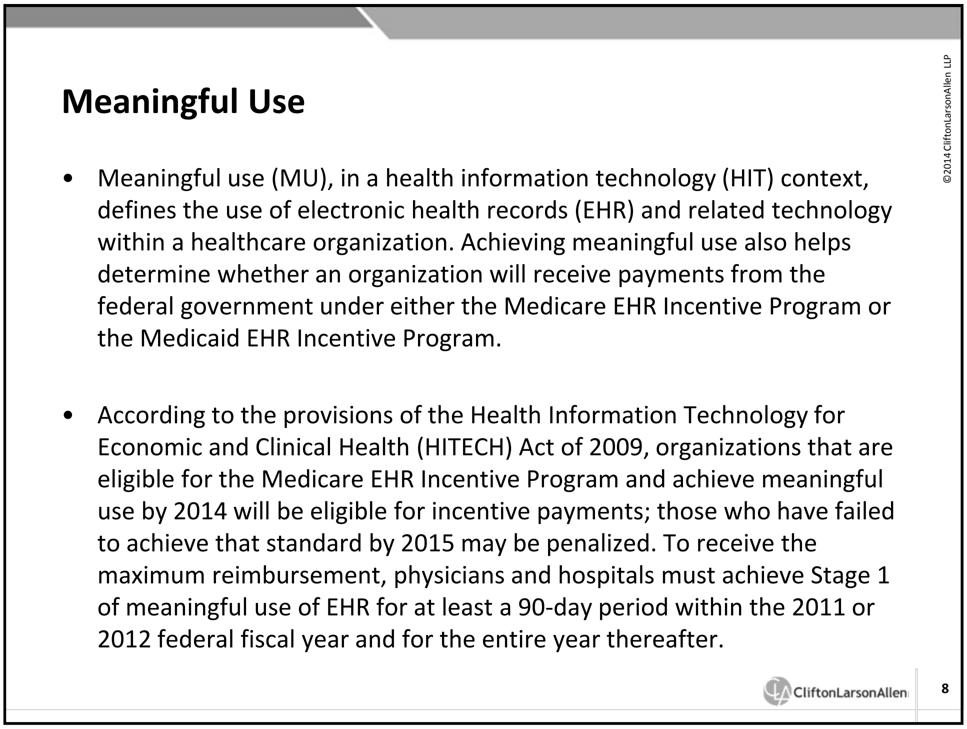


Understand what meaningful use is and how it affects HIPAA



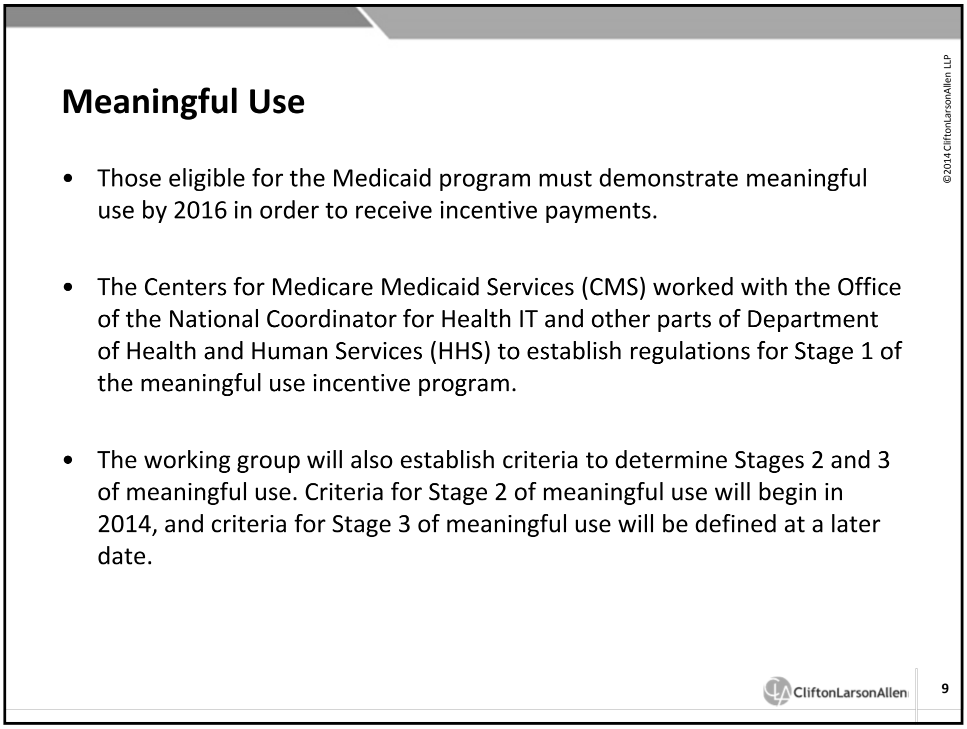
Meaningful Use

- The enhanced set of protections finalized in the omnibus HIPAA privacy and security rule now becomes the new baseline for anyone who handles health information.
- It does not change meaningful use requirements, but combined, the two may drive more providers to protect patient data.



Meaningful Use

- Meaningful use (MU), in a health information technology (HIT) context, defines the use of electronic health records (EHR) and related technology within a healthcare organization. Achieving meaningful use also helps determine whether an organization will receive payments from the federal government under either the Medicare EHR Incentive Program or the Medicaid EHR Incentive Program.
- According to the provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, organizations that are eligible for the Medicare EHR Incentive Program and achieve meaningful use by 2014 will be eligible for incentive payments; those who have failed to achieve that standard by 2015 may be penalized. To receive the maximum reimbursement, physicians and hospitals must achieve Stage 1 of meaningful use of EHR for at least a 90-day period within the 2011 or 2012 federal fiscal year and for the entire year thereafter.

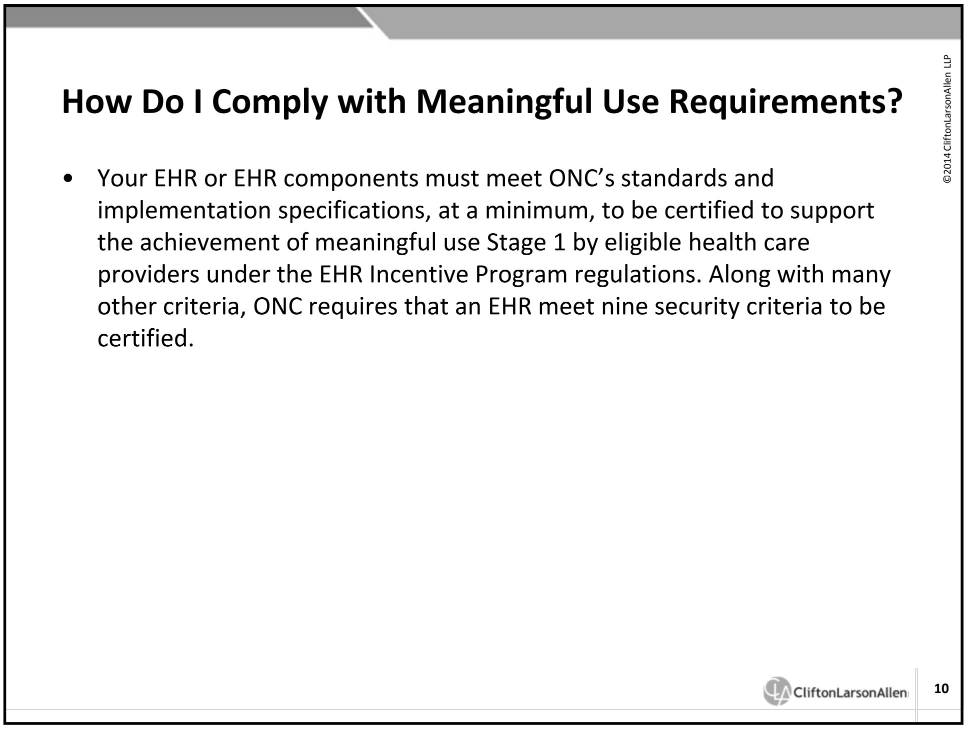


Meaningful Use

- Those eligible for the Medicaid program must demonstrate meaningful use by 2016 in order to receive incentive payments.

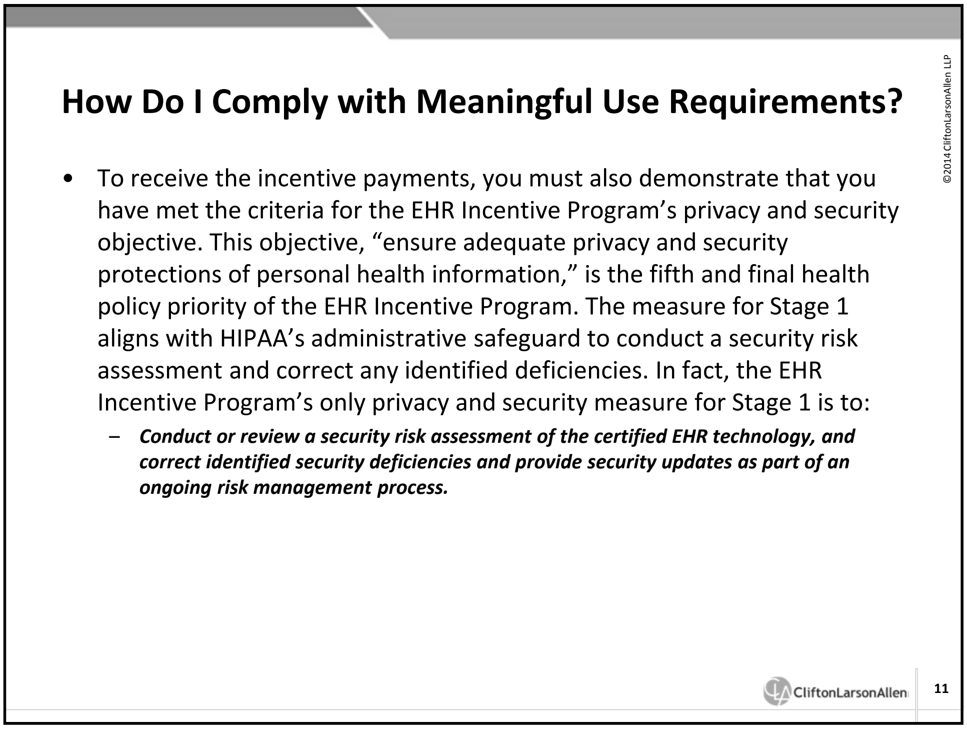
- The Centers for Medicare Medicaid Services (CMS) worked with the Office of the National Coordinator for Health IT and other parts of Department of Health and Human Services (HHS) to establish regulations for Stage 1 of the meaningful use incentive program.

- The working group will also establish criteria to determine Stages 2 and 3 of meaningful use. Criteria for Stage 2 of meaningful use will begin in 2014, and criteria for Stage 3 of meaningful use will be defined at a later date.



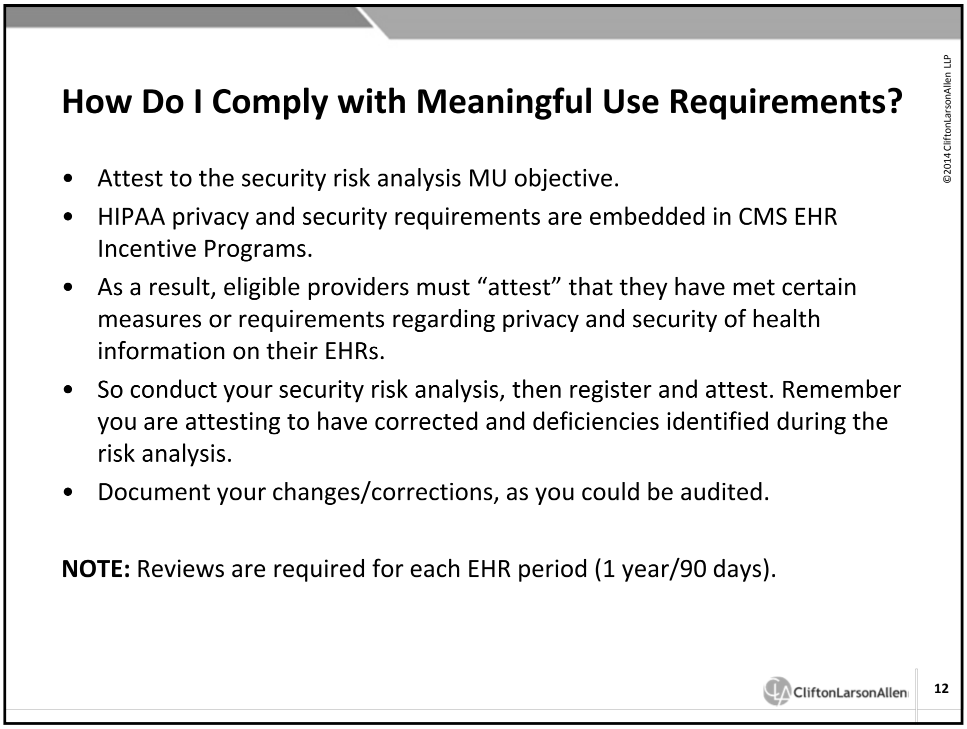
How Do I Comply with Meaningful Use Requirements?

- Your EHR or EHR components must meet ONC’s standards and implementation specifications, at a minimum, to be certified to support the achievement of meaningful use Stage 1 by eligible health care providers under the EHR Incentive Program regulations. Along with many other criteria, ONC requires that an EHR meet nine security criteria to be certified.



How Do I Comply with Meaningful Use Requirements?

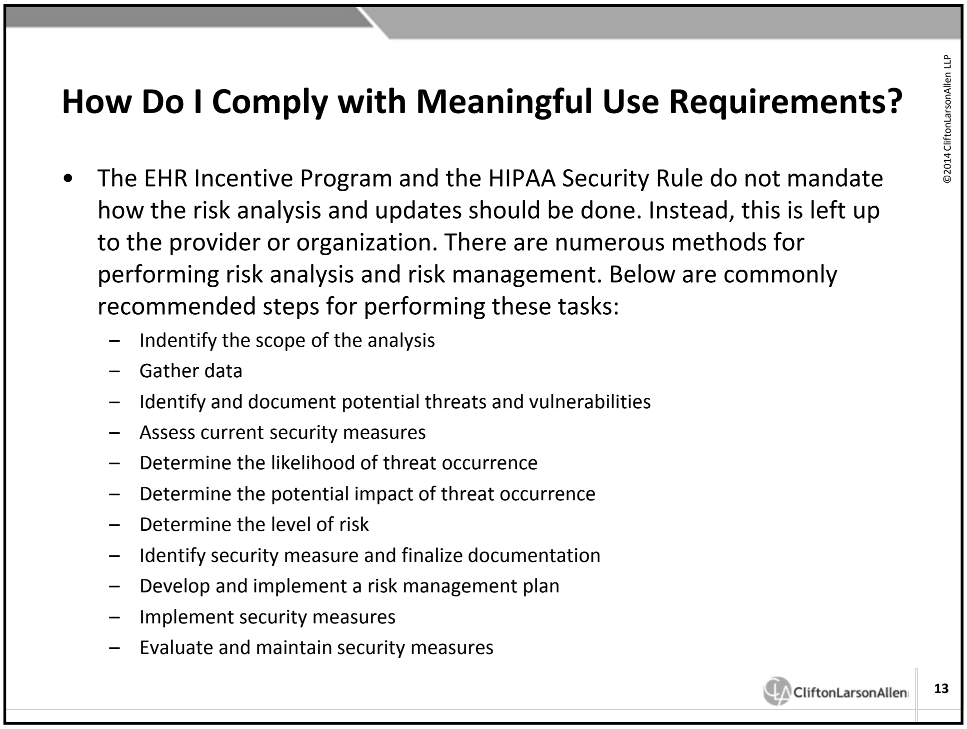
- To receive the incentive payments, you must also demonstrate that you have met the criteria for the EHR Incentive Program's privacy and security objective. This objective, "ensure adequate privacy and security protections of personal health information," is the fifth and final health policy priority of the EHR Incentive Program. The measure for Stage 1 aligns with HIPAA's administrative safeguard to conduct a security risk assessment and correct any identified deficiencies. In fact, the EHR Incentive Program's only privacy and security measure for Stage 1 is to:
  - ***Conduct or review a security risk assessment of the certified EHR technology, and correct identified security deficiencies and provide security updates as part of an ongoing risk management process.***



How Do I Comply with Meaningful Use Requirements?

- Attest to the security risk analysis MU objective.
- HIPAA privacy and security requirements are embedded in CMS EHR Incentive Programs.
- As a result, eligible providers must "attest" that they have met certain measures or requirements regarding privacy and security of health information on their EHRs.
- So conduct your security risk analysis, then register and attest. Remember you are attesting to have corrected and deficiencies identified during the risk analysis.
- Document your changes/corrections, as you could be audited.

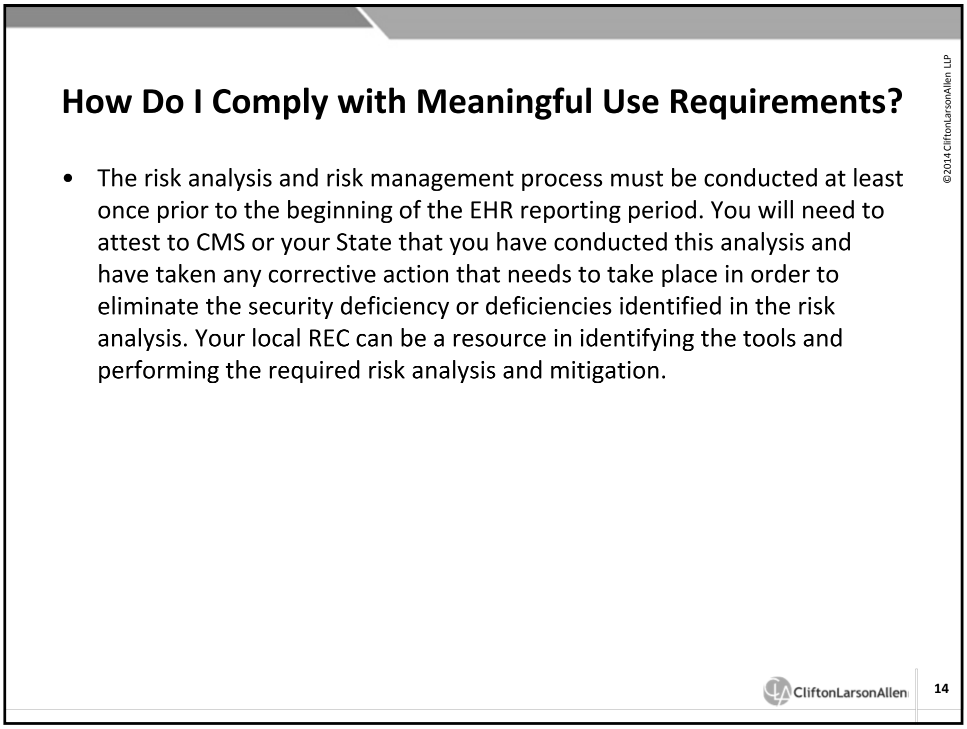
NOTE: Reviews are required for each EHR period (1 year/90 days).



How Do I Comply with Meaningful Use Requirements?

- The EHR Incentive Program and the HIPAA Security Rule do not mandate how the risk analysis and updates should be done. Instead, this is left up to the provider or organization. There are numerous methods for performing risk analysis and risk management. Below are commonly recommended steps for performing these tasks:
  - Indentify the scope of the analysis
  - Gather data
  - Identify and document potential threats and vulnerabilities
  - Assess current security measures
  - Determine the likelihood of threat occurrence
  - Determine the potential impact of threat occurrence
  - Determine the level of risk
  - Identify security measure and finalize documentation
  - Develop and implement a risk management plan
  - Implement security measures
  - Evaluate and maintain security measures

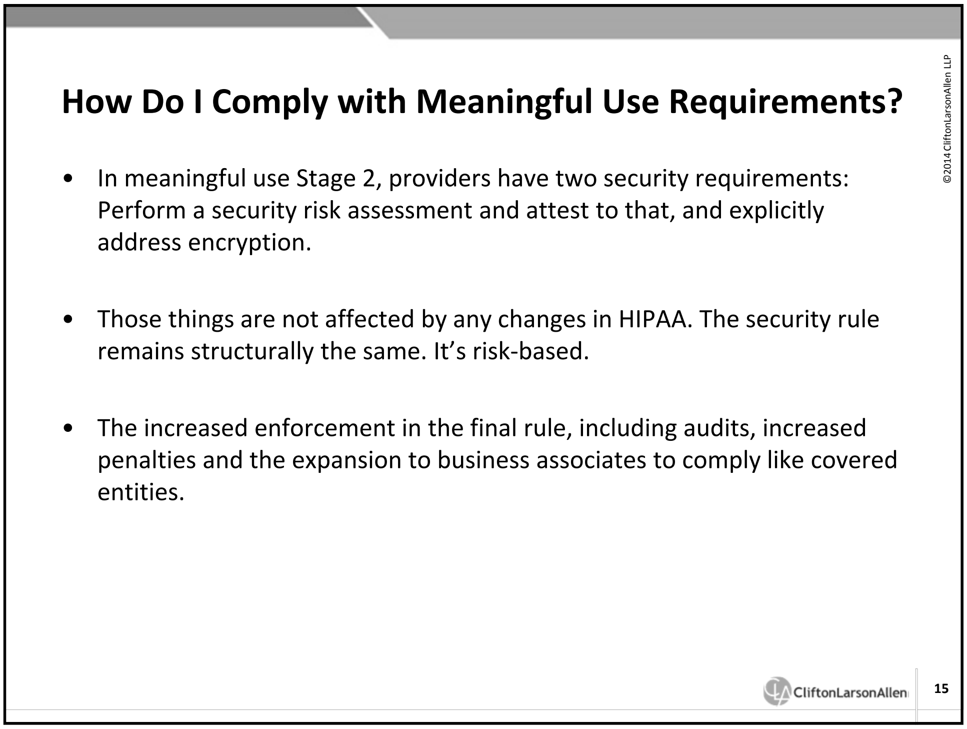
CliftonLarsonAllen



How Do I Comply with Meaningful Use Requirements?

- The risk analysis and risk management process must be conducted at least once prior to the beginning of the EHR reporting period. You will need to attest to CMS or your State that you have conducted this analysis and have taken any corrective action that needs to take place in order to eliminate the security deficiency or deficiencies identified in the risk analysis. Your local REC can be a resource in identifying the tools and performing the required risk analysis and mitigation.

CliftonLarsonAllen

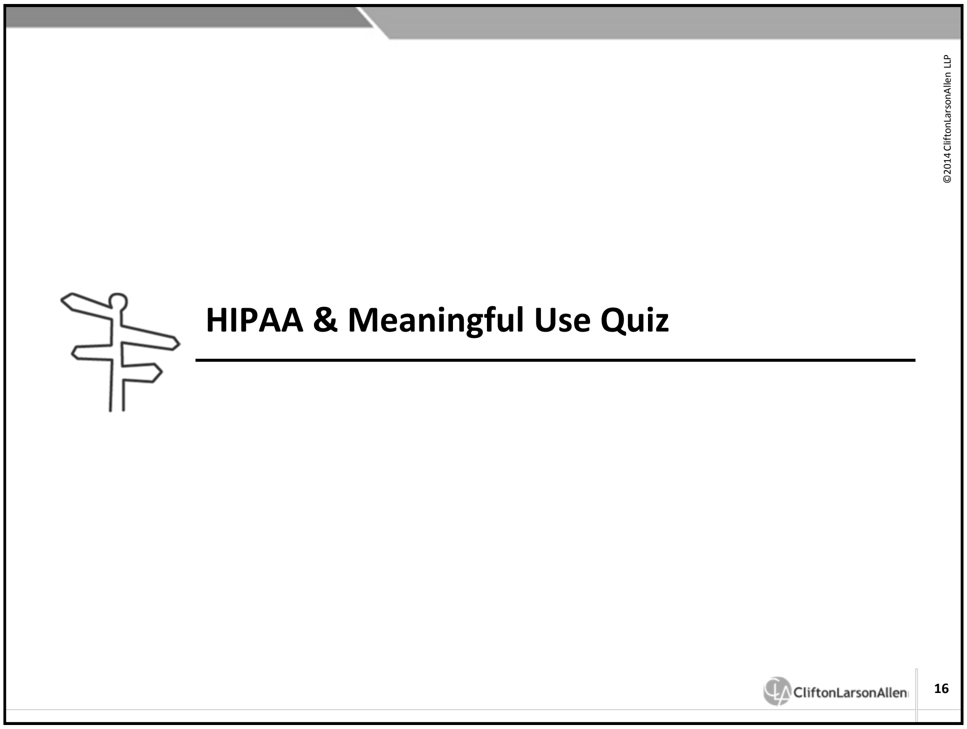


How Do I Comply with Meaningful Use Requirements?

- In meaningful use Stage 2, providers have two security requirements: Perform a security risk assessment and attest to that, and explicitly address encryption.
- Those things are not affected by any changes in HIPAA. The security rule remains structurally the same. It's risk-based.
- The increased enforcement in the final rule, including audits, increased penalties and the expansion to business associates to comply like covered entities.

CliftonLarsonAllen

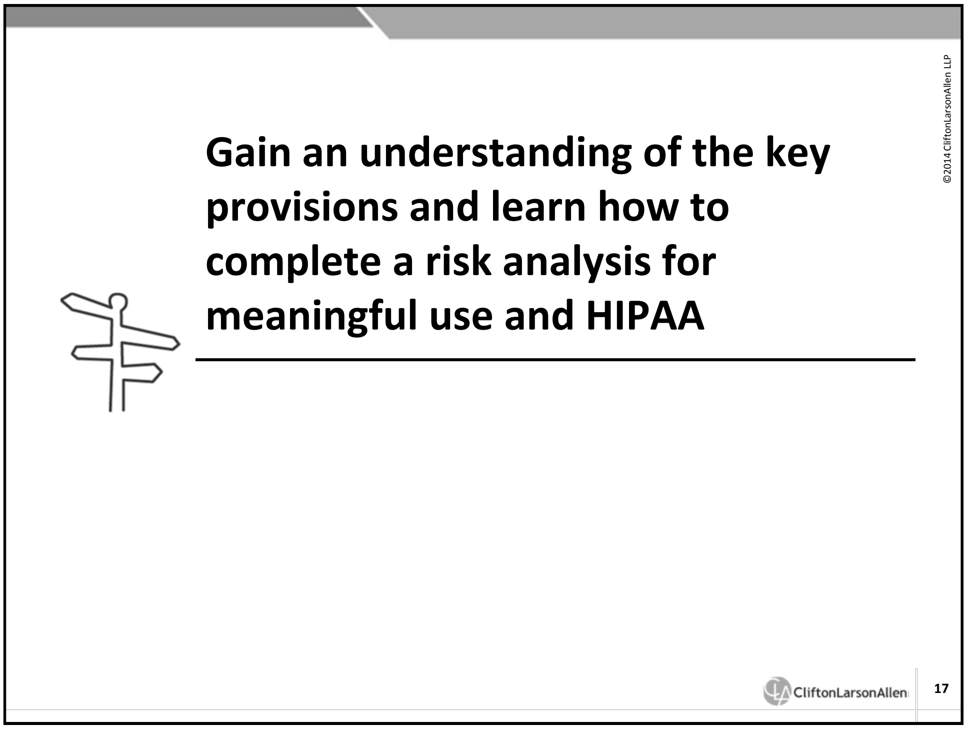
15



HIPAA & Meaningful Use Quiz

CliftonLarsonAllen

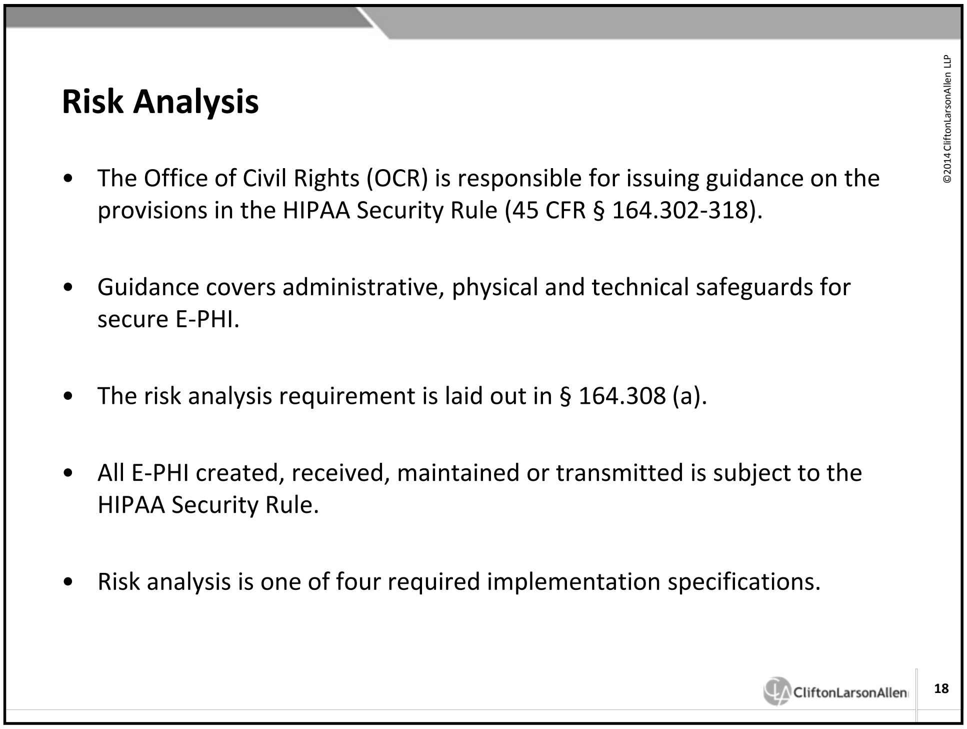
16



Gain an understanding of the key provisions and learn how to complete a risk analysis for meaningful use and HIPAA

CliftonLarsonAllen

17

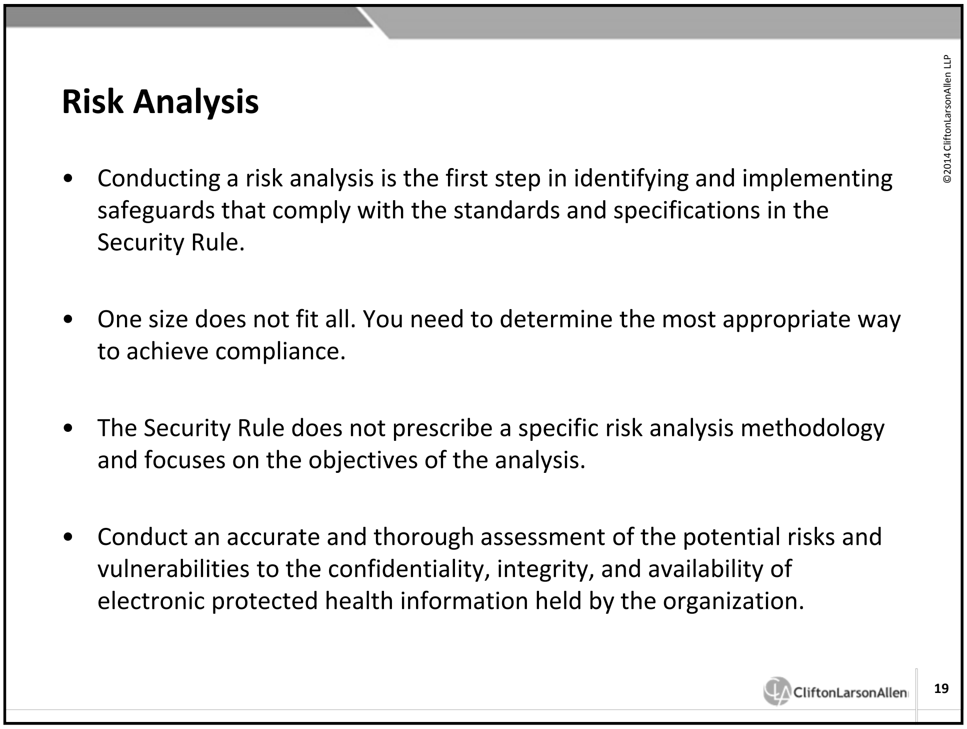


Risk Analysis

- The Office of Civil Rights (OCR) is responsible for issuing guidance on the provisions in the HIPAA Security Rule (45 CFR § 164.302-318).
- Guidance covers administrative, physical and technical safeguards for secure E-PHI.
- The risk analysis requirement is laid out in § 164.308 (a).
- All E-PHI created, received, maintained or transmitted is subject to the HIPAA Security Rule.
- Risk analysis is one of four required implementation specifications.

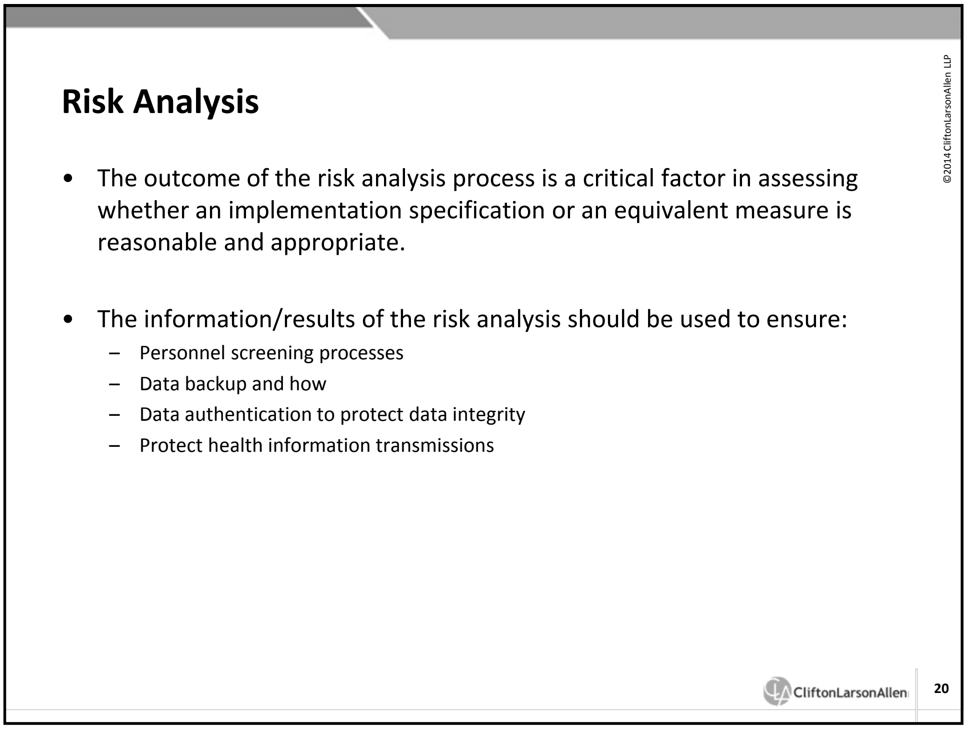
CliftonLarsonAllen

18



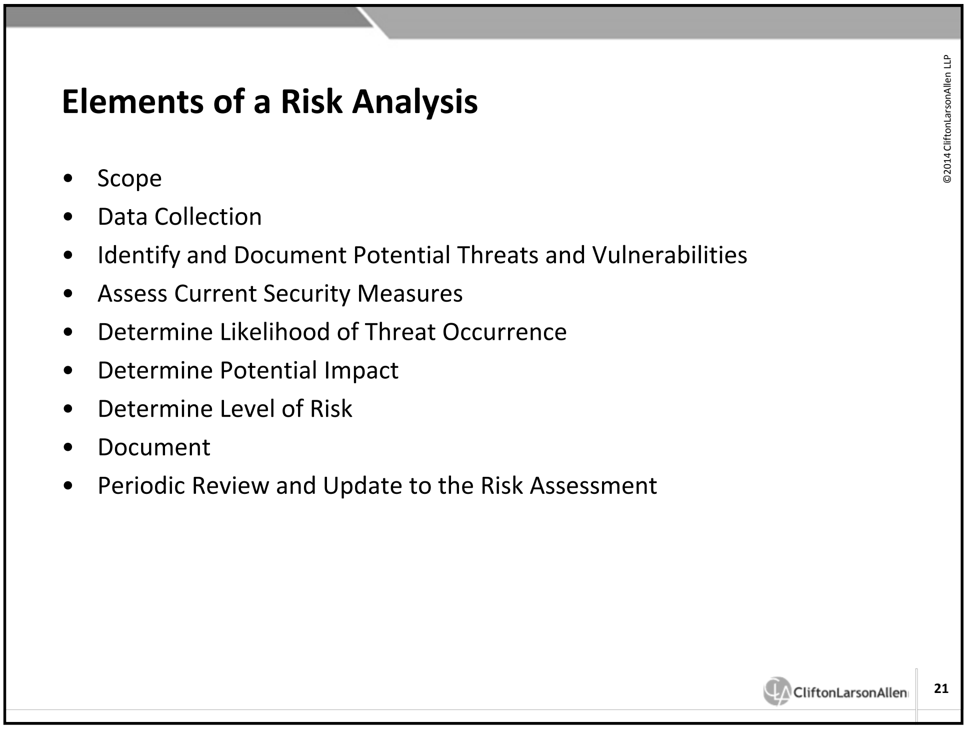
Risk Analysis

- Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with the standards and specifications in the Security Rule.
- One size does not fit all. You need to determine the most appropriate way to achieve compliance.
- The Security Rule does not prescribe a specific risk analysis methodology and focuses on the objectives of the analysis.
- Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the organization.



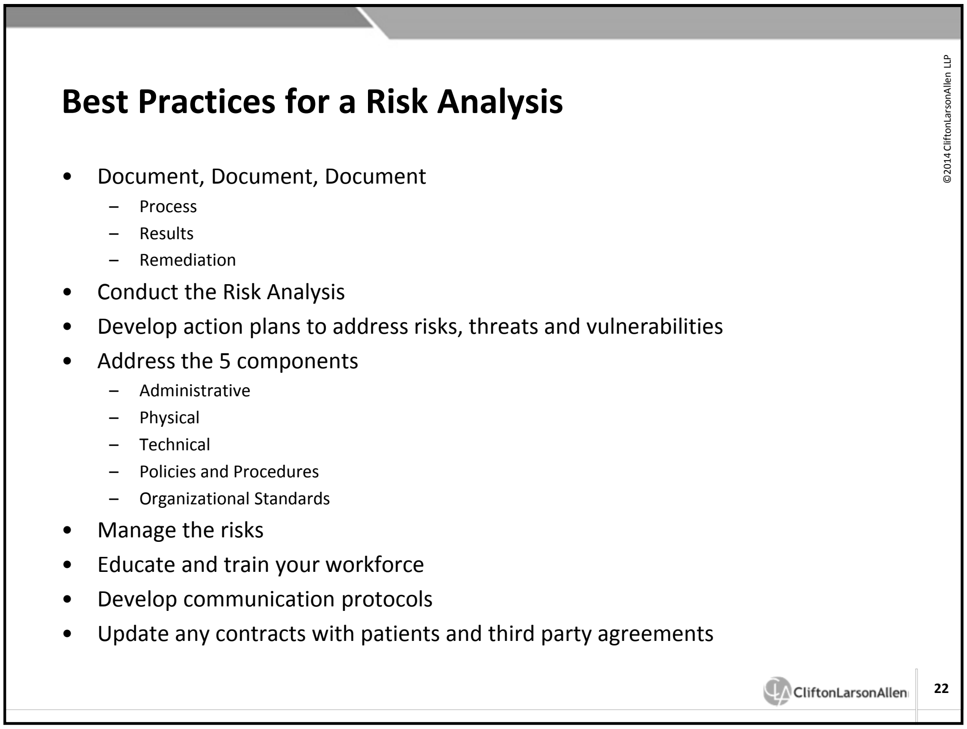
Risk Analysis

- The outcome of the risk analysis process is a critical factor in assessing whether an implementation specification or an equivalent measure is reasonable and appropriate.
- The information/results of the risk analysis should be used to ensure:
  - Personnel screening processes
  - Data backup and how
  - Data authentication to protect data integrity
  - Protect health information transmissions



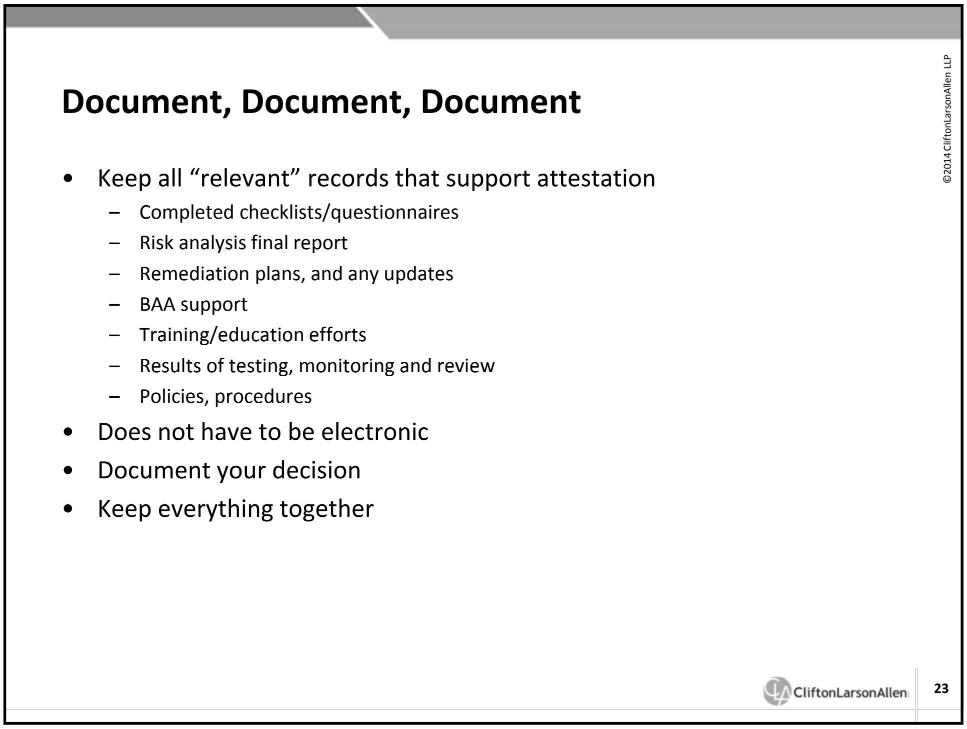
Elements of a Risk Analysis

- Scope
- Data Collection
- Identify and Document Potential Threats and Vulnerabilities
- Assess Current Security Measures
- Determine Likelihood of Threat Occurrence
- Determine Potential Impact
- Determine Level of Risk
- Document
- Periodic Review and Update to the Risk Assessment



Best Practices for a Risk Analysis

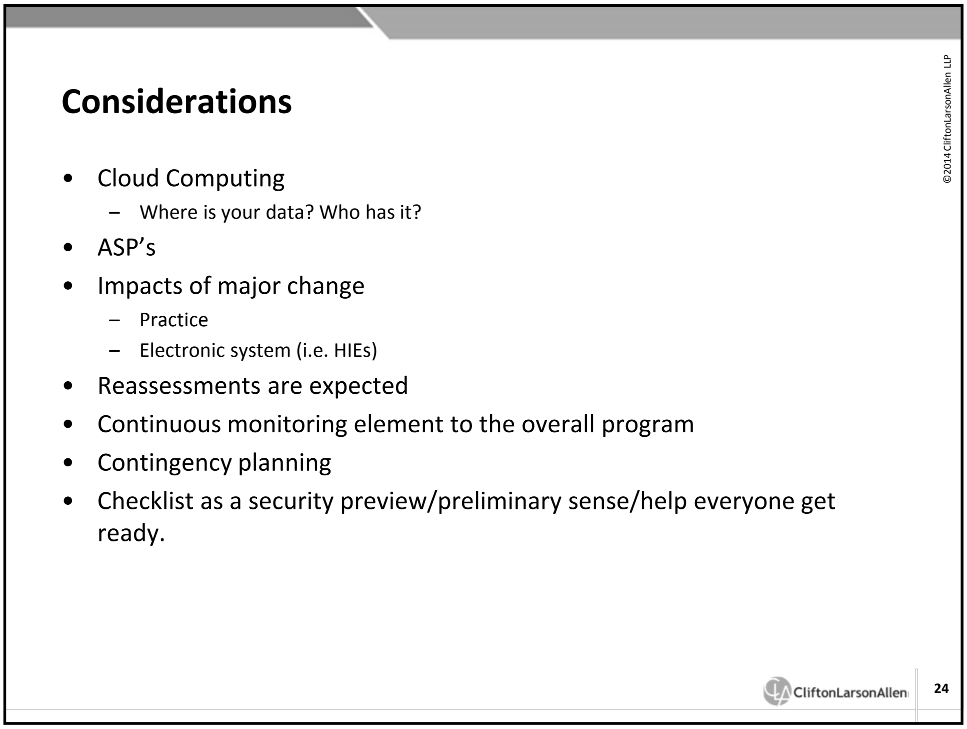
- Document, Document, Document
  - Process
  - Results
  - Remediation
- Conduct the Risk Analysis
- Develop action plans to address risks, threats and vulnerabilities
- Address the 5 components
  - Administrative
  - Physical
  - Technical
  - Policies and Procedures
  - Organizational Standards
- Manage the risks
- Educate and train your workforce
- Develop communication protocols
- Update any contracts with patients and third party agreements



Document, Document, Document

- Keep all “relevant” records that support attestation
  - Completed checklists/questionnaires
  - Risk analysis final report
  - Remediation plans, and any updates
  - BAA support
  - Training/education efforts
  - Results of testing, monitoring and review
  - Policies, procedures
- Does not have to be electronic
- Document your decision
- Keep everything together

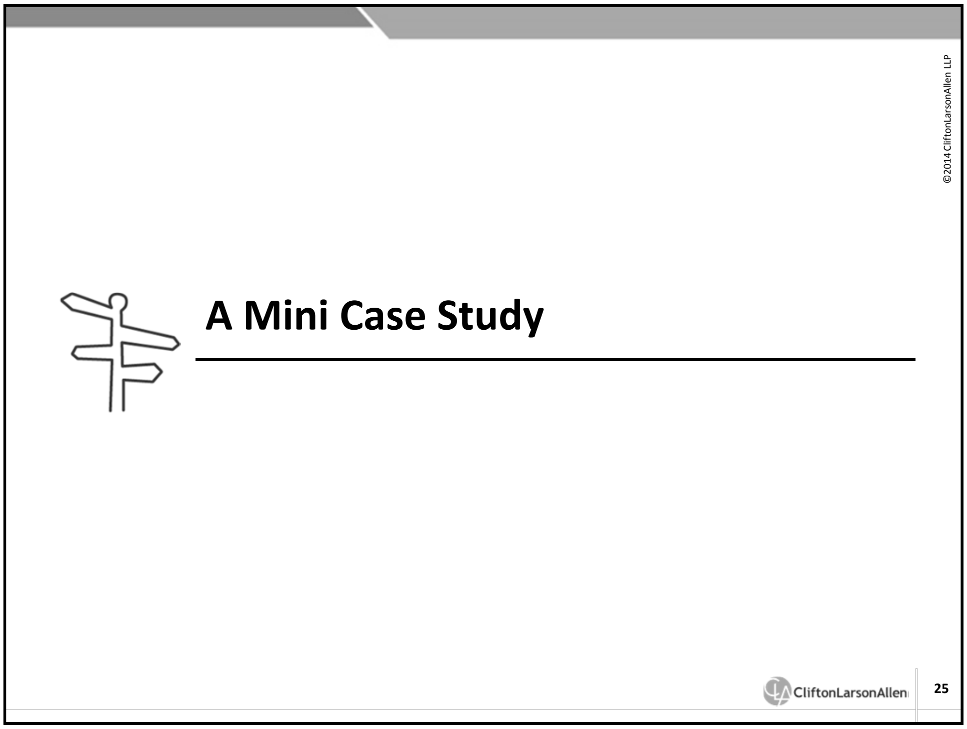
CliftonLarsonAllen 23



Considerations

- Cloud Computing
  - Where is your data? Who has it?
- ASP’s
- Impacts of major change
  - Practice
  - Electronic system (i.e. HIEs)
- Reassessments are expected
- Continuous monitoring element to the overall program
- Contingency planning
- Checklist as a security preview/preliminary sense/help everyone get ready.

CliftonLarsonAllen 24

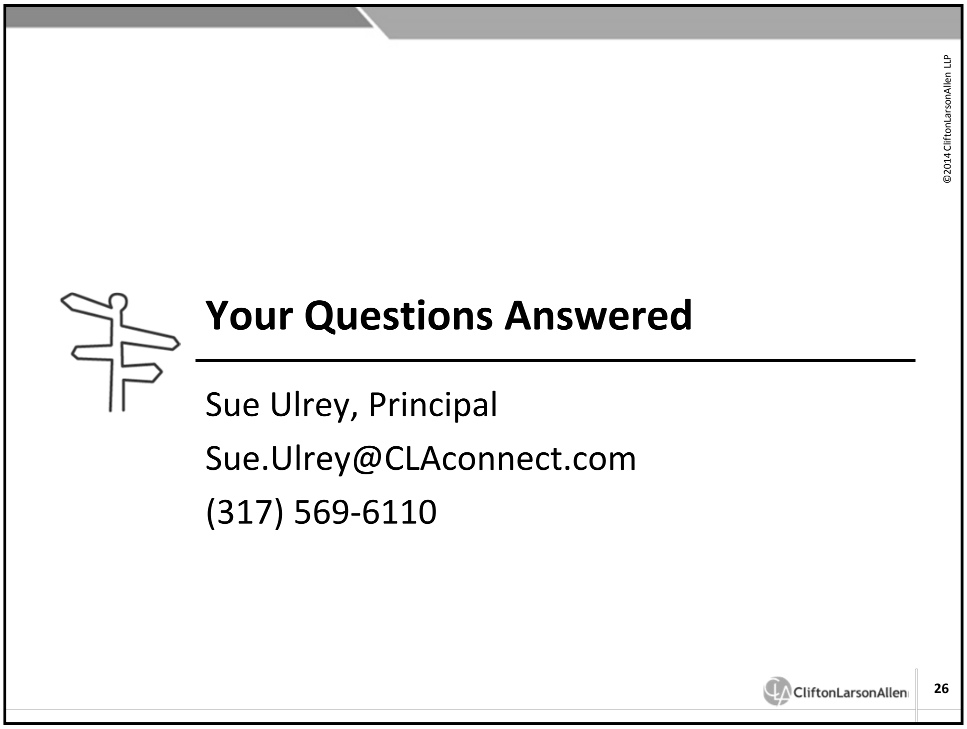


©2014 CliftonLarsonAllen LLP

A Mini Case Study

CliftonLarsonAllen

25



©2014 CliftonLarsonAllen LLP

Your Questions Answered

Sue Ulrey, Principal

Sue.Ulrey@CLAconnect.com

(317) 569-6110

CliftonLarsonAllen

26