NBI: HIPAA Requirements

HIPAA
Health Insurance Portability
& Accountability Act

Presented by

Lisa English Hinkle, Esq.
McBrayer, McGinnis, Leslie & Kirkland, PLLC

Responsive 24/7

McBRAYER
McBrayer, McGinnis, Leslie & Kirkland, PLLC

ATTORNEYS AT LAW

HIPAA Language 101

- **Office for Civil Rights (OCR)**: Tasked with overseeing and enforcing HIPAA
- **Privacy Rule**: 45 C.F.R. § 164.500 *et seq.*
- **Security Rule**: 45 C.F.R. § 164.300 *et seq.*
- **Breach Rule**: 45 C.F.R. § 164.400 *et seq.*
- **Covered Entity (CE)**: Health care provider, health plan (*e.g.*, insurance), or health care clearinghouse
  - Examples: Hospitals, nursing homes, surgery centers, physician offices, dentists, health insurance companies

HIPAA Privacy 101

- **Protected Health Information (PHI)**: Any information relating to past, present, or future physical or mental health or condition of an individual.
  - Medical records
  - Any information that identifies an individual as a patient
  - Correspondence
  - If in doubt, treat it as PHI.
- **Use** (internal) vs **Disclosure** (external)
- Minimum necessary
  - o Role based access
  - o Limit amount of PHI disclosed
- Authorization
- Data use agreement for

Limited Data Set

When Does HIPAA Apply?

Usually applies:

- Patient information from a hospital
- Medical files from a physician
- Enrollee's information from a health plan
- Nursing home resident's records
- Claims records from a health care billing company

HIPAA Language 101

- **Business Associate (BA)**:
  - A person who creates, receives, maintains, or transmits PHI on behalf of a covered entity or organized health care arrangement for a function or activity regulated by HIPAA
    - Claims processing or administration; Data analysis, processing or administration; Utilization review; Quality assurance; Patient safety activities; Billing; Benefit management; Practice management; Repricing
  - A person who provides any of the following services ***to or for a covered entity*** or organized health care arrangement where the provision of the service involves the disclosure of protected health information from the covered entity or the organized health care arrangement or from another Business Associate:
    - Legal; Actuarial; Accounting; Consulting; Data aggregation; Management; Administrative; Accreditation; Financial
  - A subcontractor (**Sub-K**) that creates, receives, maintains, or transmits protected health information on behalf of the Business Associate

HIPAA Language 101

- **Business Associate (BA) cont'd**:
  - A person becomes a Business Associate by definition, not just by the act of contracting with a covered entity or otherwise
  - **General Rule**: A Covered Entity may disclose PHI to a Business Associate in accordance with a Business Associate Contract (**BAC**)
    - CE is required to have a BAC with the Business Associate
- More on this later

HIPAA PRIVACY BASICS – Patient Rights

- Notice of Privacy Practices § 164.520
- Right to Request Restrictions/Privacy Protections § 164.522
    - Right to restrict disclosure to Insurers when pay out of pocket
- Access to PHI § 164.524
- Amendment of PHI § 164.526
- Accounting of Disclosure § 164.528
- Marketing restrictions
- Parental rights
- Right to complain

ppr

patientprivacyrights

HIPAA PRIVACY BASICS – Types of Disclosures

- **General Rule**: A Covered Entity (or Business Associate) may not use or disclose an individual’s PHI without that individual's authorization, except as permitted by HIPAA

Permitted Disclosures

- Disclosures to the Individual & HHS
- Disclosures for Treatment, Payment, & Health Care Operations (TPO Disclosures)
- Disclosures to Personal Representatives
- New Rule in the Omnibus Rule – CE must comply with HIPAA for a deceased individual for 50 years after the individual's death
- Disclosures Requiring an Authorization
- Disclosures for Facility Directories & Family
- Disclosures for Public Health, Oversight, Legal

HIPAA PRIVACY BASICS

- Establishes rules on how Covered Entities (and their business associates) may ***use and disclose*** PHI
- Grants ***patient***s certain ***rights*** with regard to their own PHI
- Imposes requirements on Covered Entities to ***safeguard*** the ***privacy*** of PHI

HIPAA PRIVACY BASICS – Administrative Requirements

- Personnel Designations
- Training
- Safeguards
- Handling Individual Complaints
- Sanctions
- Mitigation of Violations
- Refraining from Intimidating or Retaliatory Acts
- Prohibition on Waiver of Rights to Complain to HHS
- Policies and Procedures; Documentation

HIPAA SECURITY BASICS

- Requires Covered Entities/Business Associates to protect the storage and transmission of ***electronic*** PHI.

- Requires Covered Entities/Business Associates to implement ***administrative, technical and physical safeguards*** to protect electronic PHI.

- "**Required**" vs "**Addressable**" implementation specifications

- Reality: do not treat electronic and non-electronic PHI differently.
  - When is it electronic?
  - Print electronic material

HIPAA SECURITY BASICS

- Administrative safeguards (45 CFR §164.308)
  - 9 Standards
- Physical safeguards (45 CFR §164.310)
  - 4 Standards
- Technical safeguards (45 CFR §164.312)
  - 5 Standards
- Documentation (45 CFR §164.316)

Security Rule Compliance

- Technical, physical and administrative safeguards
  - Appointment of a "Security Official"
  - Security reminders
  - Policies and procedures
  - Training

- Risk analysis
  - Risk assessment
  - BA should be required to perform regular risk assessments too

Target breach involved a hacker using contractor's employees info to get in through a back door

Safeguards for Data

- The HIPAA Security Rule requires appropriate administrative, physical and technical safeguards to ensure the **confidentiality**, **integrity**, **and security** of electronic protected health information.
- **Security** encompasses all of the administrative, physical, and technical safeguards for an information system through the use of **people**, **processes**, and **technology**.

Administrative Safeguards for Data

- Have a point of contact (or contacts) security issues, handling, and coordination.
- Implement policies and procedures to prevent, detect, contain and correct security violations: Risk analysis, Risk management, Sanction policy, and Information system activity review
  - Risk analysis -- "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information…." – and manage the risks as reasonable and appropriate for your organization.
  - Apply appropriate sanctions against workforce members re: violations of organization's policies and procedures
  - Information system activity review (e.g., audit logs, access reports, and security incident tracking reports)

Administrative Safeguards for Data (con't)

- Workforce security: make sure your workforce members have appropriate access
- Implement policies and procedures for authorizing access to workforce members consistent with the Privacy Rule
  - Limit unnecessary or inappropriate access to and disclosure of protected health information
- Security awareness and training
- Security incident procedures
- Contingency plan

Administrative Safeguards for Data (con't)

- Implement ongoing monitoring and evaluation plans (Are the policies, procedures, and plans adequate?) Should be revised based upon experience?
- Have written contracts (or other written arrangements) with downstream subcontractors, as applicable.

When Does HIPAA Not Apply?

Usually doesn't apply:

- OSHA records
- Life insurance
- An individual client's personal medical data (e.g. medical malpractice plaintiffs or estate planning clients)
- Education/FERPA records
- De-identified information
- Employment / personnel records

Administrative Safeguards for Data – Practical Tips

- Consider having an acceptable use policy which sets forth what authorized users can and cannot do with your organization's IT assets, mobile devices, etc.
- Have security awareness and training for new users and continuing users regarding policies and procedures.
- Have appropriate sanctions and other measures in place in the event of a violation of policies and procedures. Know what is going on in real-time (be proactive).
- Inventory who has access to your data.

Administrative Safeguards for Data – Practical Tips (con't)

- Have a plan in place to ensure that your operations continue (and that you have your client data) even in the face of an abnormal condition or event.
- Have a plan in place for backups and disaster recovery.
- Have a plan in place to respond to incidents (identify, respond, mitigate/remediate).
- If critical IT assets go down, the plan should address how IT operations will continue (including access to the data).
- Secure the human: have controls in place prior to employment, during employment, and after termination or other change in employment).

Physical Safeguards for Data – Practical Tips

- Safeguard your facilities and your IT assets to ultimately protect your client data (i.e., control access, prevent theft and tampering, etc.)
- Have controls in place to prevent unauthorized access to facilities (e.g., card access).
  - Make sure your data center is secure.
- Make sure that workstations, laptops, mobile devices, etc., are secured, as appropriate.
- Keep records of who accesses your facilities when they access them (including guests and visitors).

Physical Safeguards for Data – Practical Tips

- Be concerned not only with unauthorized access by OUTSIDERS, but
- also with INSIDERS. The insider is someone we have given legitimate access to information, systems, and resources.
  - The insider may be an employee, intern, volunteer, security guard, janitor, contractor, consultant, etc. – essentially, anyone with inside (and authorized) access.

Technical Safeguards for Data

- **Access control for electronic information systems.** Implement technical policies and procedures for information systems with regard to authorized users and software programs.
- **Keep user and transaction logs and analyze these logs.** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems.
- **Maintain data integrity.** Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.
- **Authentication.** Implement procedures to verify that a person or entity seeking access is the one claimed.

Technical Safeguards for Data (con't)

- **Transmission security.** Implement technical security measures to guard against unauthorized access to information that is being transmitted over a network.

Technical Safeguards for Data – Practical Tips

- Make sure your network infrastructure is secure (e.g., wireless networks, routers, firewalls, etc.).
- Disable, as appropriate, automatic "joining" of networks (e.g., evil twin).
- Wired communications are generally more secure than wireless communications.

- Consider restricting access to websites and installation/use of certain applications (e.g., peer to peer sharing sites, etc.).
- Beware of Bring Your Own Device (BYOD)
  - Consider restricting installation of applications on mobile phones (e.g., flashlight applications, games, etc.) to help prevent data leakage and unwanted data exfiltration.
- Ensure secure remote access from home or on the road and mobile device security too .
- Do run antivirus/antimalware programs and regularly update definitions on your information systems (including mobile devices).
- Encrypt whenever possible data at rest, data in motion, and archived data.

- Ensure that the users accessing your resources are who they say they are.
  - Use unique user IDs (or other means of user identity proofing) for each user.
  - Use complex passwords or an appropriate alternative for authentication.
  - Track use of system to identify cases where access keys have been stolen
  - Monitor access by contractors
- Protect documents and storage media (including flash drives, backup tapes, mobile devices, and cloud) from theft, unauthorized disclosure, modification, removal, and destruction.
- Ensure appropriate disposal of all information systems and storage media.
  - This may even include photocopiers, mobile devices, and other information systems which are used either on premises or off premises (e.g., laptop computer used for work from home).

- Manage mobile and cloud assets/resources.
- Carefully evaluate any third party to whom you are outsourcing any relevant IT resources/services (e.g., backups, client portals, etc.) and ensure appropriate security measures are in place.

What Constitutes a "Breach"?

- Under the HIPAA Omnibus Rule, the acquisition, access, use, or disclosure of PHI in a manner not permitted under subpart E [the Privacy Rule] is generally ***presumed to be a breach*** unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised.
- A "security incident" includes "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."

Electronic Communication

- Reasonable safeguards for emails with PHI (encrypt, password protected)
- Careful with communication with patients
- Take steps to prevent unintentional disclosures (check email address, alerts before sending email)
- Minimum necessary
- Policies and procedures controlling access, protecting integrity, and protecting against unauthorized access to ePHI

Is it Excluded from Being a "Breach"?

Good faith:

- "The acquisition, access, or use by a workforce member or person acting under the authority of a…business associate was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part."

Inadvertent Disclosure:

- "Any inadvertent disclosure by a person who is authorized to access protected health information at a…business associate to another person authorized to access protected health information at the same…business associate,…and the information received…is not further used or disclosed in a manner not permitted under subpart E of this part."

Good faith belief not reasonably able to retain:

- A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information

Breach – Factors for Assessing Risk

The risk must be assessed using at least the following four factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

Recent Data Security Breaches

- The data security breaches at Anthem, Sony, Home Depot, and Target serve as stark reminders that all organizations, even the ones with most secure networks, face significant cybersecurity threats and challenges that could cause substantial financial costs and reputational damage.

Anthem Inc. Security Breach

- On February 4, 2015, the second largest healthcare insurance company in the U.S., Anthem Inc., reported a data security breach affecting 78.8 million customers.

- In January, hackers sent phishing emails to employees that allowed the hackers to steal at least five employees' network credentials, usernames, and passwords. These hackers even obtained the information belonging to the system administrator account. The system administrator did not notice the breach until someone used his access codes and information and was inside the system.

- Although the final report on the Anthem data breach has not yet been issued, **the fact that the hackers obtained five sets of access keys or credentials (log in and passwords) from authorized users indicates how dangerous an innocent mistake, such as opening a phishing email, can be to an entire data system.**

Target Security Breach

- During the 2013 holiday shopping season, Target suffered a substantial security breach of its credit and debit card system that impacted 70 million customers.

- The hackers obtained access to customer information through hacking Fazio Mechanical, a refrigeration **contractor of Target**. An employee of Fazio Mechanical opened a malicious phishing email that installed a piece of malware, which recorded login credentials and gave the hackers access to a portal into Target's internal systems. The hackers used the portal access to gain control of Target's servers. Thus, the hackers gained access to Target's system by hacking into the system of an outside contractor and using that contractor's access information to get into Target's system.

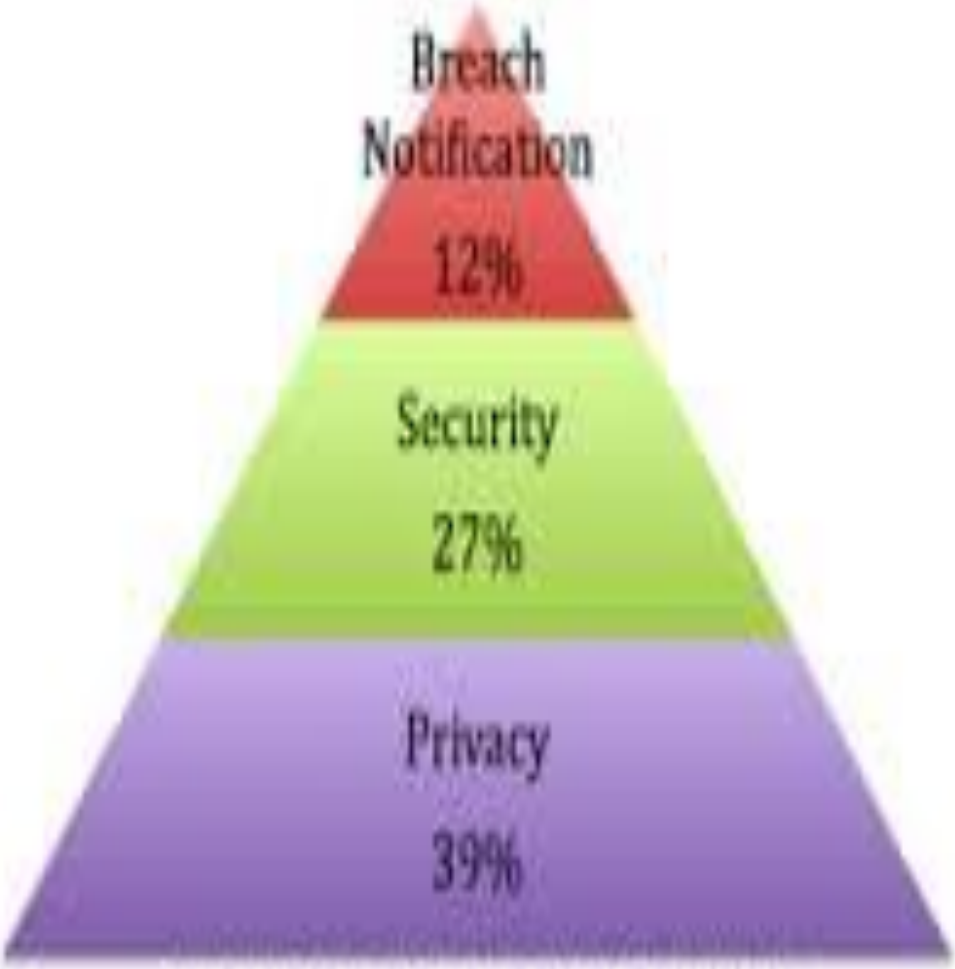
- **The Target breach indicates that covered entities must closely monitor the security breaches of their contractors, because those outside security breaches can give hackers an indirect access point or back door into the covered entity's system.**

Lessons Learned

- Train employees to detect scams and report possible scam emails'
- Test employees' ability to recognize scams
- Monitor employee access to identify stolen access info
- Limit third party and contractor's employees' access to system
- Monitor breaches of contractors to avoid back door entry
- Require that contractors assess and closely monitor security risks
- Require immediate notification of any security breach of a contractor's system

HITECH Drastically Changed OCR'S Enforcement and Auditing of HIPAA Compliance

- HIPAA Omnibus Rule formalized HITECH Act requirements and underscores the need for strengthening HIPAA compliance
- Numerous $100k+, even million-dollar penalties
- Not limited to big institutions – also includes smaller groups
- Strengthening Audit Program
- Criminal Penalties exist
- State Attorneys General can bring civil action
- No private right of action for HIPAA damages, but may be state tort liability



PERCENTAGE OF TOTAL AUDIT FINDINGS DUE TO LACK OF AWARENESS

Source: OCR March 7, 2013

HITECH /HIPAA Omnibus Rule (September 23, 2013 Compliance Date)

- HIPAA Omnibus Rule substantially strengthens HIPAA enforcement rule and incorporates increased monetary penalty tiered structure
- Incorporates and clarifies HITECH's direct regulation of "business associates" and their "subcontractors"
  - ***Direct application of HIPAA Privacy Rule to Business Associates***
  - ***Direct application of HIPAA Security Rule safeguard and documentation provisions***
- Presumes all incidents are security breaches
- Significant revisions to the breach notification rule

Enforcement and Penalties

USDHHS Office of Civil Rights (OCR) May Investigate Compliance

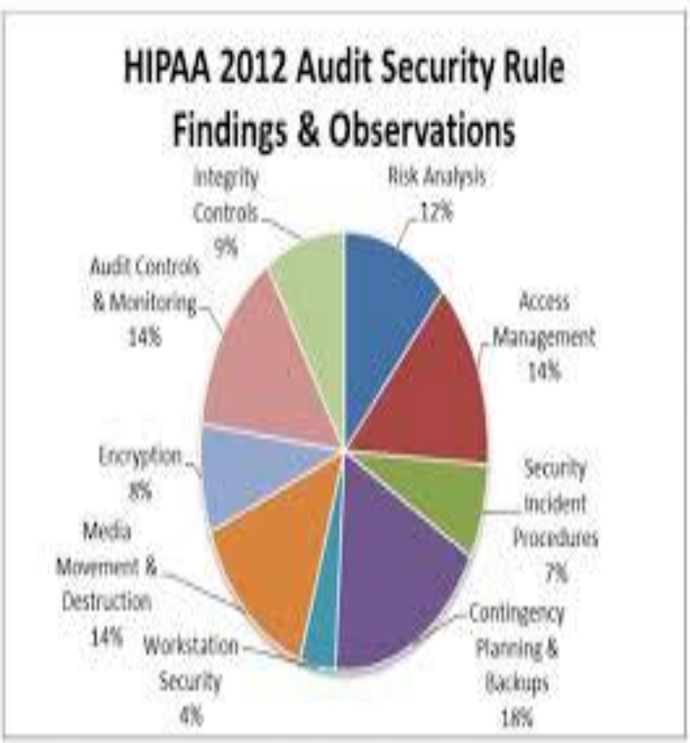
- Based on complaint by any one – whistle blower, adversary, etc.
- On OCR's own initiative; "Audit Program" contemplates audit of 1,200 Covered Entities and Business Associates
- Every notification of breach affecting 500 or more individuals is reviewed for potential investigation
- Notification of breach affecting fewer than 500 individuals may also trigger investigation

Enforcement(con't)

Scope of OCR Investigation

- Essentially unlimited as relevant to HIPAA/HITECH compliance
  - Privacy and security policies and procedures, security analyses, responses to individual requests and complaints, incident responses and breach assessments, etc.
  - Documentary records, interviews with appropriate personnel, etc.
- Covered Entities and Business Associates have regulatory obligations to maintain documentation, cooperate with investigations
  - ***Cignet Health***: Failure to cooperate with OCR investigation grounds for
- $3 million civil monetary penalty

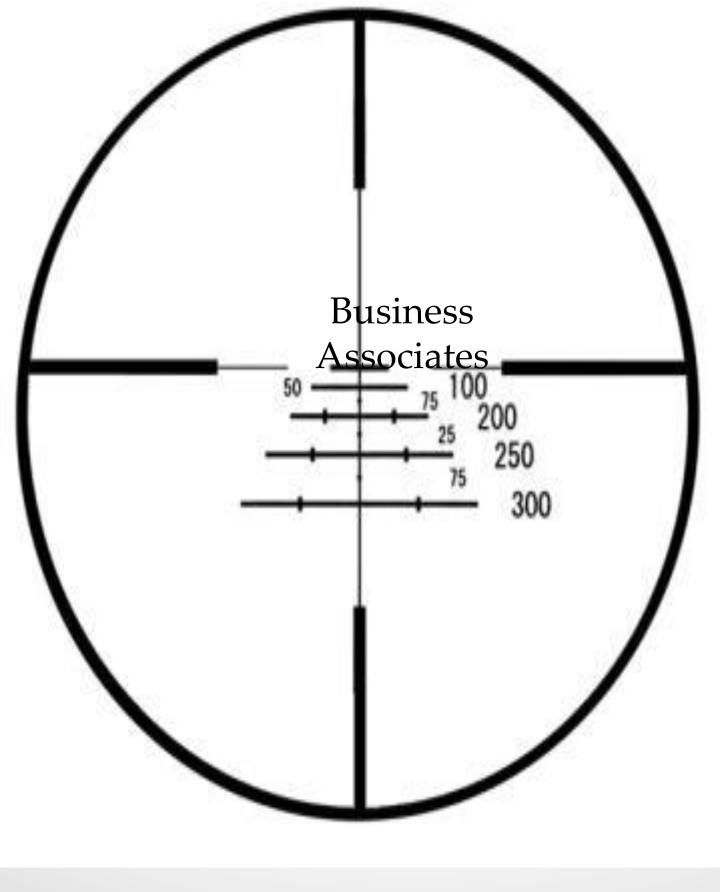
Enforcement(con't)



- 2012 HIPAA Pilot Audit
- Privacy Rule
- Security Rule
  - Incomplete Risk Analyses
  - Improper Media Disposal
  - Inadequate Access Controls
- Administrative Failures
  - Lack of training
  - Failure to update policies
  - Complete and Accurate Risk Assessment
- Leon Rodrigues reported that CE entities in the pilot program often conducted a "shallow risk assessment… with any business change, an entity must review its risk analysis; yet, two-thirds of pilot participants—including 80% of providers—did not have a complete and accurate risk analysis." AHLA Email Alert—March 14, 2014

Enforcement(con't)

- As of February 28, 2014:
  - Complaints Filed = 92,975
  - Cases Investigated = 32,227
  - Cases with Corrective Action = 22,222
  - CMP's and Resolution Agreements = >$16 million
  - Increased Authority to Issue CMP's directly against BAs



Enforcement (con't)

- HITECH drastically changed enforcement and auditing authority of OCR
- OCR TO BEGIN SECOND ROUND OF HIPAA AUDITS
- March 14, 2014 OCR announced that it is gearing up for second round of audits by starting with a survey of 1200 organizations including 400 business associates.
- Survey: "gather information about the respondents to enable OCR to assess the size, complexity and fitness of a respondent for an audit."

HIPAA
HITECH
COMPLIANT

Enforcement(con’t)

Key Civil Monetary Penalty (“CMP”) Concepts

- May be imposed upon Covered Entities (your client) and Business Associates (you), and upon both if both are found at fault
- Calculated at one violation per failure to comply with any “requirement” (positive or negative obligation) of the Privacy or Security Rule
- One failure can violate more than one requirement
- “Continuing violation:” Any requirement whose failure “continues” from the time at which the violation first began
  - Counted at one violation per day, for each day it “continues”
- Foundational violation: Any failure to comply with a requirement which causes failures to comply with other requirements

Enforcement(con't)

Potential CMP Amounts

- Violation not known (despite due diligence): $100/violation to $25,000 calendar year maximum
- Violation due to "reasonable cause:" $1,000/violation to $100,000 calendar year maximum
- Violation due to "willful neglect:" Increased to $500,000/violation to
- $1.5 million calendar year maximum

Lisa English Hinkle, Esq.
McBrayer, McGinnis, Leslie
& Kirkland, PLLC
201 East Main Street, Suite 900
Lexington, Kentucky 40507
(859) 231-8780
lhinkle@mmlk.com

Responsive 24/7

McBRAYER
McBrayer, McGinnis, Leslie & Kirkland, PLLC

ATTORNEYS AT LAW