HIPAA: What Lawyers Need to Know

Presented by

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

HIPAA: Why Should You Care?

HIPAA applies to me? I am a lawyer and I have ethical duties…

McBRAYER

Why Should Lawyers Care about HIPAA/HITECH and the Regulations?

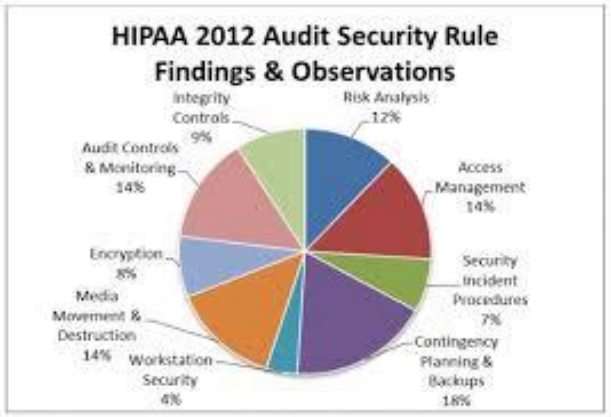
- Lawyers often must have Protected Health Information to perform their jobs
- Lawyers qualify as Business Associates when a client discloses/authorizes use of Protected Health Information
- HITECH drastically expanded the enforcement and auditing authority of Office of Civil Rights ("OCR")

Why Should Lawyers Care about HIPAA/HITECH and the Regulations?

- The Omnibus Final Rule makes Business Associates directly liable for
  - Impermissible uses and disclosures of PHI
  - Failure to notify Covered Entity when PHI is lost or inappropriately accessed
  - Failure to provide electronic PHI when requested
  - Failure to disclose PHI when requested by CMS to investigate BA's compliance
  - Failure to provide accounting of disclosures
  - Failure to comply with the Security Rule

Why Should Lawyers Care about HIPAA/HITECH and the Regulations? (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

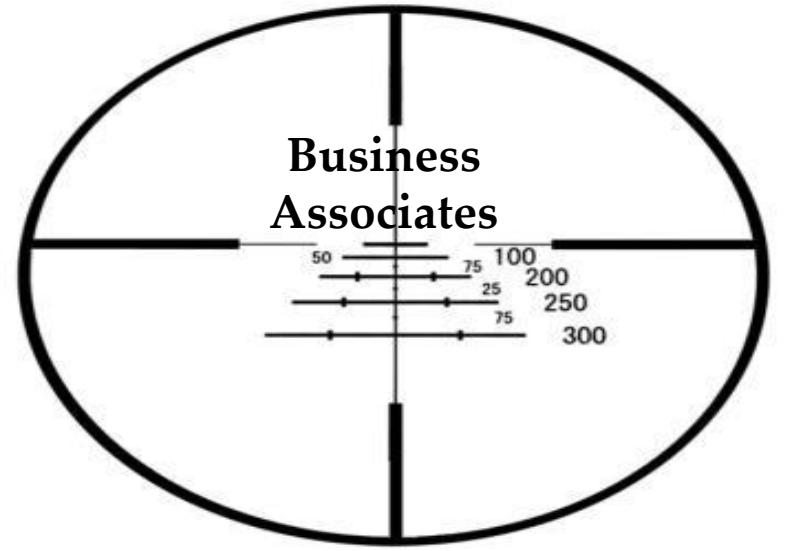


HITECH

Changed the Landscape for Lawyers

- HIPAA Omnibus Rule formalized HITECH Act Numerous $100k+, even million-dollar penalties
- Not limited to big institutions – also includes smaller groups
- OCR can audit law firms as BAA
- Criminal Penalties exist
- State Attorneys General can bring civil action
- No private right of action for HIPAA damages, but may be state tort liability

- 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



McBRAYER

Penalty Tier	Business Associate's Culpability Level	Penalty Per Incident
Tier 1*	Did not know and could not have known of the HIPAA violation.	$100 – $50,000
Tier 2*	Knew, or would have known through reasonable due diligence that an act or omission violates HIPAA, but did not act with willful neglect.	$1,000 – $50,000
Tier 3	Acted with willful neglect, but corrected the violation within 30 days	$10,000 – $50,000
Tier 4	Acted with willful neglect and took no corrective actions within 30 days.	$50,000
***Timely corrective action is an affirmative defense to Tier 1 and Tier 2 violations.[28]**		

What are the penalties?

- Civil Monetary Penalties can be issued against lawyers as Business Associates
- Level of culpability and remedial efforts address

HITECH Regulations/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 Business Associate provisions***
  - ***Direct application of HIPAA Security Rule safeguard and documentation provisions***
- Direct accountability to government!
- Still have to enter into Business Associate Agreements with Covered Entities
- Significant revisions to the breach notification rule

McBRAYER

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 Language 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)

McBRAYER

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 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

McBRAYER

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

McBRAYER

EXCEPTIONS

- 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

McBRAYER

HIPAA PRIVACY BASICS – Individual Rights

- Notice of Privacy Practices § 164.520
- Right to Request Restrictions/Privacy Protections § 164.522
- Access to PHI § 164.524
- Amendment of PHI § 164.526
- Accounting of Disclosure § 164.528

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)

McBRAYER

Key Business Associate Obligations

- BAs are:
  - Exposed to potential federal criminal penalties for violation of HIPAA
  - Subject to regulatory jurisdiction of OCR and state attorneys general
  - Required to cooperate with OCR investigations of CE and Bas
  - Exposed to potential civil monetary penalties for violation of HIPAA
  - Can be exposed to private tort actions by individuals harmed by BA failure to comply with HIPAA
  - Examples:
    - Walgreens Indiana Verdict: $2 million

How Law Firms Become Business Associates

- Creating, receiving, maintaining or transmitting protected health information on behalf of a "covered entity" client
- Providing services to a client that is a business associate of other covered entities can also trigger HIPAA obligations (software vendors, accountants, consultants, third party administrators)
- Receiving a client's medical records from a covered entity

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

McBRAYER

When Does HIPAA Not Usually 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

HIPAA Compliance

McBRAYER

Examples of Scenarios that May Trigger Business Associate Obligations

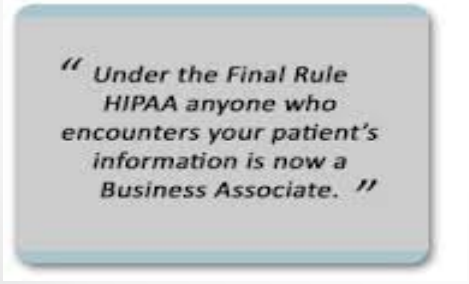
- Physician contacts you to defend her in a medical malpractice action where you will need to review her records.
- Hospital contacts you to provide advice regarding an unpaid patient bill.
- Nursing home asks you to interview residents regarding an adverse incident.
- Billing company calls with a regulatory question and asks you to review claims.

Examples of Scenarios that Probably Don't Trigger Business Associate Obligations

- Pharmacy asks you to review its policies and procedures. (No PHI)
- Employer asks you to help determine whether an employee is entitled to family medical leave.
- A life insurance company or workers' comp plan asks you to defend it in a suit brought by an insured.
- An individual injured in an automobile accident asks you to file a lawsuit.
- An estate planning client asks you to draft a health care power of attorney. (No PHI)

What HIPAA Requires of Law Firm Business Associates

- Protection of health information in accordance with HIPAA Security Rule and "business associate agreements"
- Business associate agreements
  - Require specific provisions
  - Agreements that were in effect and in compliance with HIPAA as of January 25, 2013 generally need to be amended by September 22, 2014
  - Other agreements should have been amended by September 23, 2013



McBRAYER

10 Things a Business Associate (BA) Agreement Must Address

- Establish the permitted and required uses and disclosures of PHI by BA
- Provide that BA will not use or further disclose the information other than as permitted or required by the contract or as required by law
- Require the BA to implement appropriate safeguards to prevent unauthorized use or disclosure of the PHI, including compliance with the Security Rule for ePHI

What a BA Must Contain (con't)

- Require reporting to Covered Entity any improper use or disclosure, including breaches
- Require BA to make PHI available for access and amendment, and require information for accounting
- Require Privacy Rule compliance, to the extent applicable
- Require BA to make books and records available to HHS – *Don't forget about the attorney/client privilege!*

What a BA Must Contain (con't)

- Require return or destruction of PHI at termination, if feasible
- Require the BA to ensure that subcontractors agree to the same restrictions and conditions
- Authorize termination of the contract by CE if the BA violates a material term

These agreements involve serious ethical considerations for lawyers!

Security Rule Compliance

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

McBRAYER

Other Requirements

- Privacy and security policies and procedures
- Employee training on those policies
- Accounting of certain disclosures for purposes other than treatment, payment, and health care operations
- Documentation of satisfactory assurances from subcontractors and service providers
  - Consultants
  - Experts
  - Shredding companies
  - Document and cloud storage companies, etc.

Even if You're Not a Business Associate…

- Be aware of HIPAA's requirements for obtaining health information from covered entities
  - Specific requirements for subpoenas
  - Special requirements for authorization forms
  - State privacy laws may apply even if your client is not a covered entity
- HIPAA may apply to your firm's employee health plan

McBRAYER

Checklist for Lawyers as Business Associates

- Appoint a HIPAA Security Officer
- Identify clients to whom firm is a Business Associate
- Determine whether firm receives, transmits, or maintains PHI
- Conduct a risk analysis/assessment
- Draft and implement policies, procedures, and other documentation/practices required by the Security Rule

McBRAYER

Checklist (cont'd)

- Draft policies and procedures relating to BA obligations:
  - Reporting breaches of unsecured PHI
  - Reporting unauthorized uses and disclosures
  - Responding to requests for access/accounting
  - Identifying PHI
  - Determining when BA and subcontractor agreements may be required

Checklist (cont'd)

- Revise/draft BA and subcontractor agreement templates to reflect HITECH/Omnibus Rule changes
- Keep PHI secure (limit off-site uses, keep in files instead of out in the open, don't talk about PHI in public, address encryption)
- Disclose PHI only to those who need to know in order to perform their job function

Checklist (cont'd)

- Train law firm personnel on your HIPAA polices and procedures
- Provide periodic security reminders
- Ensure that third parties to whom you disclose PHI have executed a BA subcontractor agreement (if necessary)
- Notify Security Official of any potential breach

Safeguards for Client 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**.

HIPAA COMPLIANCE

McBRAYER

Administrative Safeguards for Client 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 Client 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 Client 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.

McBRAYER

Administrative Safeguards for Client 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 Client 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 Client 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 Client 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.

McBRAYER

Technical Safeguards for Client 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 Client Data (con't)

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

McBRAYER

Technical Safeguards for Client 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.

McBRAYER

- Consider restricting access to websites and installation/use of certain applications (e.g., peer to peer sharing sites, etc.).
- Consider restricting installation of applications on mobile phones (e.g., flashlight applications, games, etc.) to help prevent data leakage and unwanted data exfiltration.
- 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 secure remote access from home or on the road and mobile device security too.

- 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.
- Protect documents and storage media (including flash drives, backup tapes, mobile devices, and cloud) from unauthorized disclosure, modification, removal, and destruction.
- Ensure that all information systems and storage media are appropriately disposed of.
    - 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.

McBRAYER

BA Requirements for Response and Reporting of Security Incidents

- 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."
- Business associates must "[r]eport to the covered entity any security incident of which it becomes aware[.]"
- The business associate must identify and respond to suspected or known security incidents and document the security incidents and their outcomes.
- The business associate must report security incidents to the covered entity (including those reported to it by its subcontractors).

BA Requirements for Response and Reporting of Security Incidents

- The business associate must mitigate, to the extent practicable, harmful effects of security incidents that are known to the business associate.
- The business associate must conduct a risk assessment to determine the probability that the information was compromised in view of the security incident.
- Not all security incidents rise to the level of a breach, but you may be able to prevent a breach by blocking unsuccessful attempts to infiltrate your systems or exfiltrate your data.

What Constitutes a "Breach"?

- A "breach" is generally defined as an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E [the Privacy Rule] is 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 based on a risk assessment of at least four factors.

- 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.

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.

McBRAYER

What Could Possibly Go Wrong?

Civil Monetary Penalties

"A complaint alleged that a law firm working on behalf of a pharmacy chain in an administrative proceeding impermissibly disclosed the PHI of a customer of the pharmacy chain. OCR . . . found no evidence that the law firm had impermissibly disclosed the customer's PHI. However, the investigation revealed that the pharmacy chain and the law firm had not entered into a Business Associate Agreement . . . Without a properly executed agreement, a covered entity may not disclose PHI to its law firm. To resolve the matter, OCR required the pharmacy chain and the law firm to enter into a business associate agreement."

- ***Pharmacy Chain Enters into Business Associate Agreement with Law Firm,*** hhs.gov Health Information Privacy website

What Could Possibly Go Wrong?

Major Client Financial and Reputational Harm

- ***M.O. v. Internal Medicine Associates, Inc.*** (Monroe County Circuit Court, Indiana 2013)
  - Healthcare provider retained attorney to collect patient debt.
  - Attorney's public court filings included patient name, contact information, Social Security number and positive HIV status, unsealed for six months. No evidence information was ever viewed.
  - Medical review board concluded health care provider violated the standard of care for patient privacy.
  - Jury awarded patient $1.25 million for emotional distress, embarrassment based on negligence claim.

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 and Penalties

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 and Penalties

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 and Penalties

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

McBRAYER

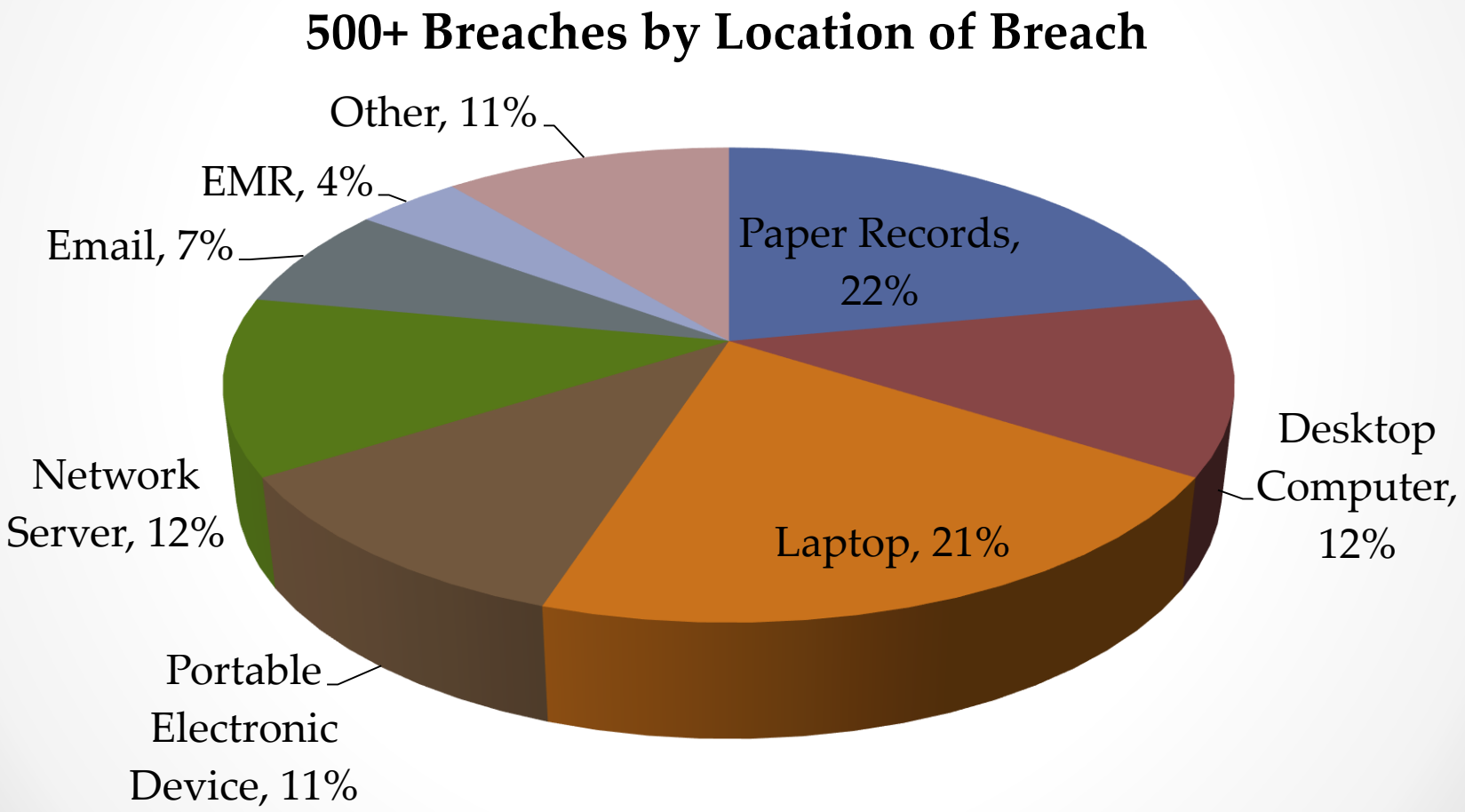
OCR Enforcement Statistics

- CY 2014 Resolution Agreements/Corrective Action Plans
  - 7 RA/CAPS
  - Total resolution amounts of $7,940,220

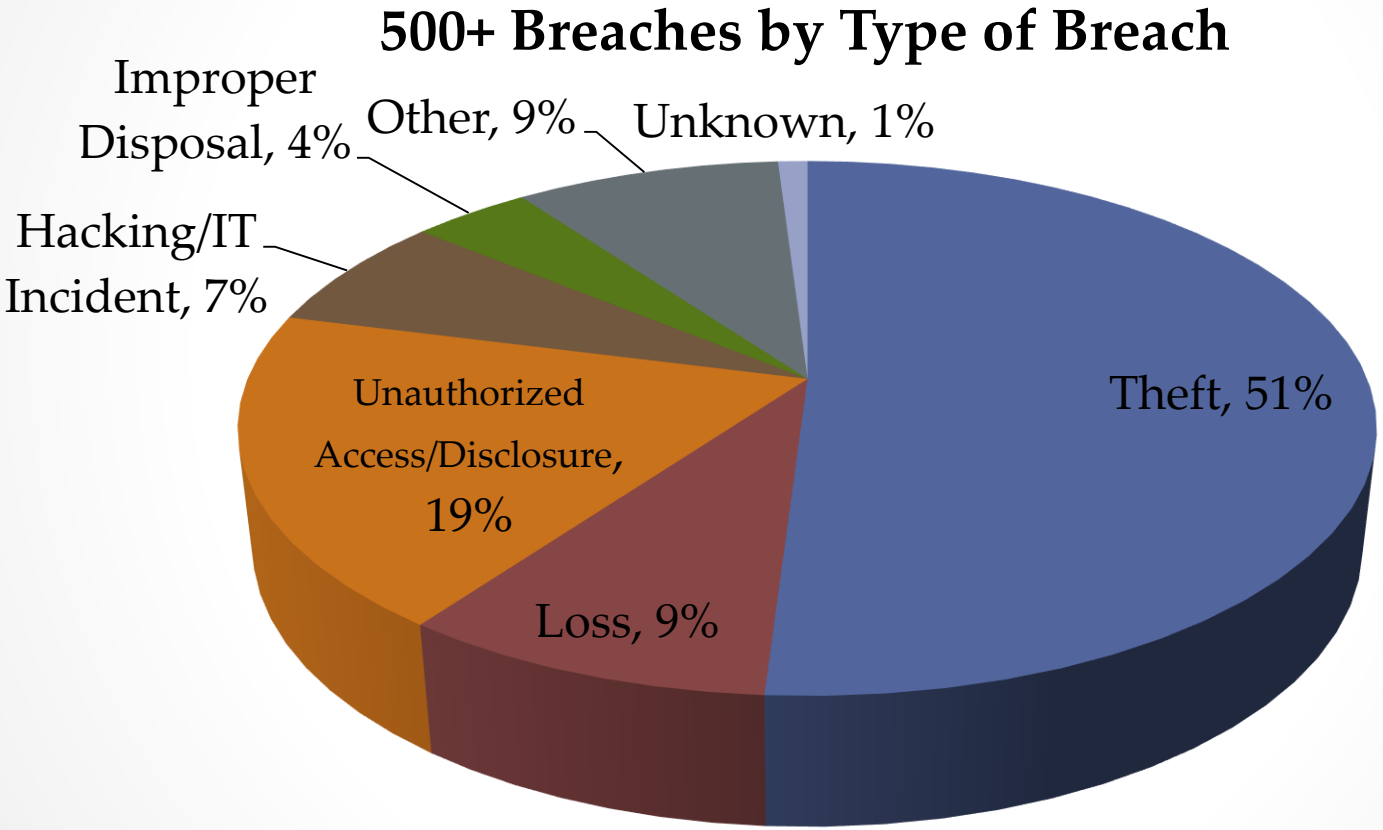
- CY 2013 Investigated Complaints/Compliance Reviews
  - 4,459 investigative closures
  - 3,467 closed with corrective action

- Breach Reports
  - 1,144 breaches involving 500 or more individuals
  - Over 157,000 breaches involving fewer than 500 individuals

Breach Notification



Breach Notification



Recent Enforcement Actions

- Cornell Prescription Pharmacy ($125,000)
  - Paper records left in an unlocked container on Cornell's premises
- Anchorage Community Mental Health Services, Inc. ($150,000)
  - Malware compromised the security of ePHI due to unpatched, unsupported software
- Parkview Health System ($800,000)
  - Parkview left 71 boxes of medical records in a retiring physician's driveway
- NY Presbyterian Hospital and Columbia University Medical Center ($4.8 million)
  - Deactivation of server resulted in ePHI of 6,800 patients being accessible on internet search engines
  - Both entities failed to conduct accurate and thorough risk analysis

Recent Enforcement Actions

- Concentra Health Services ($1,725,220)
  - Unencrypted laptop containing the ePHI of 870 individuals was stolen from one of Concentra's facilities
  - Lack of encryption identified as critical risk prior to breach incident but steps to implement were incomplete and inconsistent
- Adult & Pediatric Dermatology, P.C. ($150,000)
  - Unencrypted thumb drive containing the ePHI of approximately 2,200 individuals was stolen from an employee's vehicle
  - Failed to comply with the administrative requirements of the Breach Notification Rule
- Affinity Health Plan, Inc. ($1,215,780)
  - ePHI left on leased photocopiers when returned to leasing agents
  - 344,579 individuals affected
  - Failed to include ePHI stored on photocopier hard drives in risk analysis

State Data Breach Laws

- Kentucky is the 47th state to enact laws concerning data breach and data breach notification
- KRS 365.725 requires any business that must dispose of private customer records to take reasonable steps to destroy that information by shredding, erasing or modifying it to make it unreadable or indecipherable.
- KRS 365.730 provides a private cause of action to recover damages for violations of KRS 365.725 – *this means that there is potentially a state private cause of action to HIPAA violations*
- KRS 365.732 provides breach notification provisions, but entities to which HIPAA applies are specifically excluded by its terms

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

McBRAYER