

Lawyers as HIPAA Business Associates

**ISBA Solo and Small Firm Conference
October 4, 2013**

Rick L. Hindmand
McDonald Hopkins LLC

Background – HIPAA/HITECH Act/Omnibus Rule

Who is a business associate (BA)?

When is a lawyer or law firm a BA?

BA responsibilities under HIPAA Rules

HIPAA enforcement and lessons learned

Interplay of responsibilities under Rules of Professional Conduct (RPC) and HIPAA

Compliance steps for lawyer BAs

Health Insurance Portability and Accountability Act of 1996 (HIPAA) – administrative simplification provisions

HIPAA Rules – 45 C.F.R. Parts 160 and 164:

- Security Rule - 45 C.F.R. § 164.302 – .318
 - Administrative, physical and technical safeguards
- Privacy Rule - 45 C.F.R. § 164.500 - .534
- Breach Notification Rule - 45 C.F.R. § 164.400-.414
- 45 CFR Part 160: general, definitions & enforcement

Office for Civil Rights (OCR) – HHS agency regulating HIPAA

Protected Health Information (PHI) – individually identifiable health information

Electronic Protected Health Information (ePHI) – PHI transmitted or maintained in electronic media

~~HIPAA Background (cont'd)~~

Covered entities and business associates are subject to the HIPAA Rules

Covered Entity (CE)

- Health care provider transmitting PHI electronically
- Health plan
- Health care clearinghouse (e.g., medical billing company)

~~HIPAA Background (cont'd)~~

McDonald Hopkins LLC Attorneys at Law Chicago Cleveland Columbus Detroit Miami West Palm Beach 5

~~HIPAA Background (cont'd)~~

Business Associate (BA) – Performs services involving PHI for or on behalf of a Covered Entity

Business Associate Agreement (BAA) – written contract b/w BA and CE governing BA's use and obligations re PHI

~~HIPAA Background (cont'd)~~

McDonald Hopkins LLC Attorneys at Law Chicago Cleveland Columbus Detroit Miami West Palm Beach 6

The Health Information Technology for Economic and Clinical Health (HITECH) Act

- Part of the American Recovery and Reinvestment Act of 2009 (ARRA)
- Incentives for the use of electronic health records (EHRs)
- Extension of HIPAA obligations and liability to BAs
- Mandatory breach notification obligations for covered entities and BAs
- Increased enforcement and penalties

Omnibus Rule (overview):

- Revise Privacy, Security, Breach Notification and Enforcement Rules
- Implement HITECH changes
- Extend and expand business associate obligations
- Change the standard for determining whether breach notification obligations are triggered

	Pre-HITECH	Now
BA subject to HIPAA standards & penalties (civil and criminal)	No	Yes
Subcontractor subject to HIPAA	No	Yes
BA consequence for HIPAA noncompliance	Termination Damages	HIPAA criminal & civil penalties; damages
Maximum civil penalty/violation	\$100	\$50,000 (up to \$1.5M for identical violations in a calendar year)
CE vicarious liability for BA	No	If BA is agent of CE
Fed. breach notification obligation	No	Yes
audits – sources	Complaint or suspicion	Complaint, breach notice, periodic, meaningful use, suspicion or discretionary

McDonald Hopkins LLC Attorneys at Law Chicago Cleveland Columbus Detroit Miami West Palm Beach 9

Business Associate:

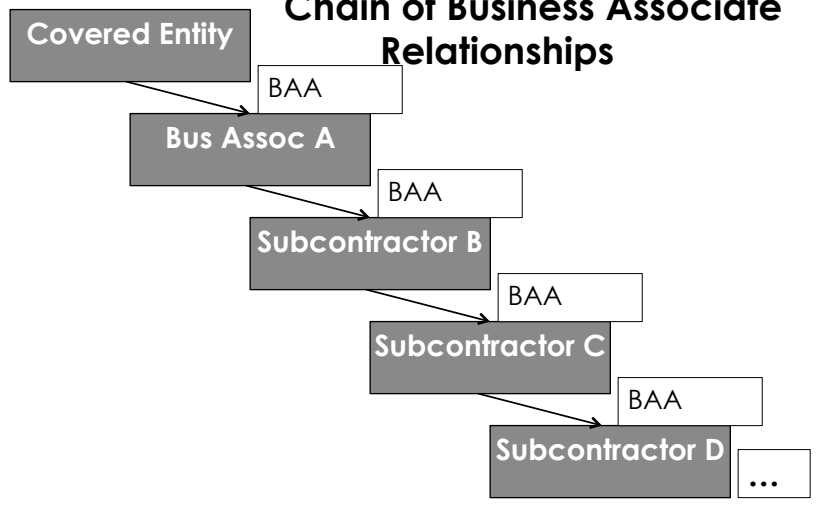
- Creates, receives, maintains or transmits PHI on behalf of a covered entity or an organized health care arrangement (OHCA) for a function or activity regulated under the HIPAA administrative simplification rules; or
- Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity, if the service involves the disclosure of PHI

McDonald Hopkins LLC Attorneys at Law Chicago Cleveland Columbus Detroit Miami West Palm Beach 10

Expansion of Business Associate definition

- Those who store or otherwise maintain PHI
- Data transmission services with routine access to PHI
- Personal health record vendors on behalf of covered entities
- Narrowing of conduit exception - courier services, such as U.S. Postal Service, UPS and their electronic equivalents that provide mere data transmission services
- Subcontractors of Business Associates

Chain of Business Associate Relationships



Typically a business associate:

- Medical transcription
- Answering service
- Document storage or disposal (e.g., shredding)
- Patient safety or accreditation
- Claims processing, repricing or collections
- Health information exchanges (HIEs), e-prescribing gateways, health information organizations (HIOs)
- Third party administrators and pharmacy benefit managers
- Data conversion, de-identification and data analysis
- Utilization review and management companies

Typically not a business associate:

- Workforce of the covered entity
- Health care provider (re disclosure for treatment)
- Plan sponsor (re disclosures from its group health plan)
- Bank (when performing only payment processing activities)
- Janitorial service
- Maintenance and repair personnel (if no PHI access)
- Conduits (e.g., U.S. Postal Service and its electronic equivalents)

Sometimes a business associate

- Accounting firm
- Auditor
- Law firm
- Consulting firm
- Software vendor or consultant
- Financial institutions (if engaging in accounts receivable or other functions extending beyond payment processing)
- ISPs, ASPs and cloud vendors
- Companies providing personal health records

Business Associate:

- Provides legal services
- For a covered entity or business associate client
 - Health care provider, health plan, health care clearinghouse
 - Employer not a covered entity, but health plan is
- Involving PHI
 - Consider whether PHI is needed.

Examples of lawyer as business associate (if access to PHI):

- Malpractice defense
- Reimbursement audits and disputes
- Internal investigation of health system
- Disciplinary actions (licensing, medical staff privileges)
- Responding to requests for medical records
- Collection for medical bills
- Breach notification and response
- Engaged as subcontractor by law firm BA

Examples of lawyer NOT a business associate :

- No access to PHI
- Workforce (e.g., in-house counsel)
- Not representing covered entity or business associate

BAA requirements:

- Permitted and required uses and disclosures of PHI
- Allow the covered entity to terminate for breach
- No use or disclosure except as provided in the BAA
- Safeguards to prevent improper use or disclosure
- Comply with the Privacy Rule
- Enter into BAAs with its downstream subcontractors at least as stringent as the upstream BAA
- (cont'd on next slide)

BAA requirements (cont'd):

- Report breaches, security incidents and improper uses or disclosures of PHI
- Make PHI available for covered entity to respond to requests from individuals
- Allow HHS access to books and records
- At termination, return or destroy PHI (if feasible)
 - Extend protections of the BAA if not feasible to return or destroy

Business associate agreements are more than mere templates

Negotiable terms include:

- Business associate right to use and disclose PHI for its management and administration
- Indemnification and insurance
- More stringent breach notification deadlines and responsibilities
- Notice and cure period
- Restriction on use of subcontractors

Omnibus Rule requires amendment of existing business associate agreements

Grandfather date (up to 9-22-14) - existing BAAs that complied with prior rules and are not renewed or modified after 3-26-13

Law firm retention of subcontractors

- Subcontractor relationship
- Business associate agreement
- Agency liability
 - Federal common law of agency
 - Right or authority to control the subcontractor's conduct
- Experts/consultants as subcontractors and agents
- Obligation to take reasonable steps to cure known subcontractor breaches or terminate

The Security Rule requires covered entities *and* business associates to implement reasonable and appropriate administrative, physical and technical safeguards

Security Rule applies to ePHI

Required v addressable safeguards

Administrative safeguards – risk analysis, risk management, regular review of system activity, security incident procedures, security officer, workforce sanction policy, workforce security, training, contingency plan

Physical safeguards – facility access controls, workstation use and security, device and media controls

Technical safeguards – access control, audit controls, integrity, user authentication, transmission security

The HITECH Act and Breach Notification Rule mandate breach notification upon discovery of unauthorized uses and disclosures of "unsecured PHI."

3 step process in determining whether a “breach” occurred

1. Use or disclosure of unsecured PHI in violation of the Privacy Rule
 - “secured” v “unsecured” PHI
 - 2 recognized methods of securing PHI:
 - Encryption – NIST
 - Destruction
2. Determine whether an exception is satisfied:
 - Unintentional, good faith acquisition, access or use by a workforce member
 - Inadvertent disclosure b/w persons with authorized access
 - Recipient unable to retain the PHI

3. Presumption of breach unless risk assessment shows low probability of compromise, based on at least the following 4 factors:
 - Nature and extent of PHI involved (e.g., types of identifiers and likelihood of re-identification)
 - Who accessed or used the PHI
 - Was the PHI acquired or viewed?
 - Mitigation – extent to which the risk has been mitigated

Notice obligation of covered entity

- To individual, media and HHS

Notice obligation of business associate

- To covered entity – without unreasonable delay and in no case later than 60 days after discovery
- Subcontractor notice obligation
- Business associate agreement may impose stricter standards

“Discovery” – earlier of actual knowledge or reasonable diligence standard

- Business associate's discovery will be imputed to the covered entity if the business associate is an agent of the covered entity

Some implications of breach:

- Transparency - notification
 - May trigger investigation
 - PR – impact on goodwill
- Expense – average data breach cost = \$7.2M and \$210 per compromised record (Ponemon Institute)
- Covered entity/business associate relationship
 - Need for coordination
 - Potential tension/finger-pointing & indemnification
- Review policies (especially Incident Response Plan)
- Mitigation and correction

Don't forget state breach notification laws

- Residence of affected individuals determines applicable notice law

Illinois Personal Information Protection Act

- Breach of the security of the system data =
 - Unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information (e.g., name + SSN, driver's license # or account access info)
- Notice of breach
 - Notify Illinois resident of breach
 - Expedient, without unreasonable delay

Phoenix Cardiac Surgery (2012)

- Small group practice – posted appointments on publicly-accessible internet-based calendar
- No risk analysis, policies & procedures
- No BAA with business associate that maintained the calendar
- \$100K fine

Affinity Health Plan (August 2013)

- Returned copiers to leasing agent without erasing hard drives
- Risk analysis
- \$1.2M fine

MA Eye and Ear Infirmary (2012)

- Theft of unencrypted laptop
- Culture of noncompliance
- No risk analysis of portable media
- \$1.5M fine

Breaches in the News (Cont'd)

BCBS Tennessee (2012)

- Theft of unencrypted computer hard drives
- Physical security, lack of encryption
- \$1.5M fine

Wellpoint (July 2013)

- PHI publicly accessible online
- Failure to update security policies and perform risk analysis upon software upgrade
- Authorization of access
- \$1.7M fine

Surgeons of Lake County (IL) (2012)

- PHI held hostage

Breaches in the News (Cont'd)

Alaska DHHS (2012)

- Stolen USB hard drive
- Lack of risk analysis
- Failure to address encryption
- \$1.7M


Hospice of North Idaho (2013)

- Stolen unencrypted laptop
- Failure to conduct risk analysis
- Lack of policy to ensure security of mobile devices
- \$50K

HIPAA Enforcement & Audits

Lessons learned from recent HIPAA enforcement activity and audits:

- Risk analysis
- Encryption
- HIPAA & HITECH policies and procedures
- Training
- Documentation
- Periodic review and update
- Don't wait until audit or investigation to adopt or update policies
- Mitigation and correction
- Cooperate if investigated



35

McDonald Hopkins LLC Chicago Cleveland Columbus Detroit Miami West Palm Beach
 Attorneys at Law

Interplay of HIPAA & Business Associate Agreements

Business Associate Agreement – RPC 1.8 and 1.4:

- RPC 1.8 – transactions with clients:
 - Fair and reasonable
 - Fully disclosed in writing
 - Informed consent
 - Right to seek advice of counsel
- RPC 1.4:
 - Explain the matter to permit informed decision


36

McDonald Hopkins LLC Chicago Cleveland Columbus Detroit Miami West Palm Beach
 Attorneys at Law

HHS access to records - RPC 1.6:

- Confidentiality
 - Informed consent; or
 - Necessary to comply with law
- RPC 1.4:
 - Explain the matter to permit informed decision
- Does HIPAA access requirement supersede RPC 1.6?
 - 2002 HHS preamble - the Privacy Rule is not intended to interfere with the attorney-client privilege (67 Fed. Reg. 53181, 53253)

Risk Analysis: assess potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI

- Data Collection - Identify (a) where ePHI is stored, received, maintained or transmitted, and (b) Information system activity
- Identify and document potential threats and vulnerabilities
- Assess and document current security measures, compliance training and adherence to policy
- Determine the probability of potential risks and the potential impact of a threat triggering or exploiting a vulnerability
- Assign risk levels for threats
- Document risk analysis
- Periodic reviews

Review and update Business Associate relationships:

- Identify all business associate relationships
- Identify subcontractor relationships
- Business associate agreements
 - Determine grandfathered status
 - Amend existing BAAs before the deadline
- Due diligence in establishing subcontractor BA relationships
 - Potential agency liability for subcontractors

Implement/update policies and procedures

- Security Rule – administrative, physical and technical safeguards
- Breach notification
- Privacy
- Coordinate policies

Training

Documentation – show your work

Take action on security gaps (risk management)

~~Other Compliance Steps (Cont'd)~~

Encrypt data (ePHI)

Avoid unnecessary access to PHI

- Deidentified PHI when feasible
- Send/request PHI only if needed

Cyber insurance

Promptly correct identified HIPAA violations

- Within 30 days after discovery - elimination or reduction of penalties

McDonald Hopkins LLC Chicago Cleveland Columbus Detroit Miami West Palm Beach Attorneys at Law 41

Questions?

Rick L. Hindmand
rhindmand@mcdonaldhopkins.com
(312) 642-2203

McDonald Hopkins LLC Chicago Cleveland Columbus Detroit Miami West Palm Beach Attorneys at Law 42

Lawyers as HIPAA Business Associates

By Rick L. Hindmand¹

Lawyers and law firms that access patient information in connection with their representation of HIPAA covered entities, such as health care providers or health plans, face substantial new obligations and potential liabilities as business associates under the final Omnibus Rule announced by the Office for Civil Rights (OCR) of the Department of Health and Human Services (HHS) on January 17, 2013. Business associates (including law firms) as well as covered entities have been required to comply with the Omnibus Rule since September 23, 2013. It is therefore crucial for lawyers to identify all of their business associate relationships and take appropriate actions to comply with the new regulations.

This outline provides background on the HIPAA Rules and discusses the HIPAA obligations of lawyer business associates and some overlapping responsibilities of lawyers under the HIPAA Rules and the Illinois Rules of Professional Conduct (RPC).

1. HIPAA Definitions. The following are some common HIPAA terms that are used within this outline:
 - a. “Breach”² means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI. Any acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule is presumed to be a Breach unless the covered entity or business associate demonstrates that there is a low probability that the PHI has been compromised, based on a risk assessment of at least the following factors: the nature and extent of the PHI, including the types of identifiers and 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. However, Breach excludes the following:
 - i. Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of the covered entity or business associate, if such acquisition, access or use 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 the Privacy Rule;
 - ii. Any inadvertent disclosure, by a person who is authorized to access PHI at the covered entity or business associate to access PHI at the same covered entity or business associate, or OHCA in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule; or

¹ Member, McDonald Hopkins LLC, Chicago, IL rhindmand@mcdonaldhopkins.com

² 45 C.F.R. § 164.402.

- iii. A disclosure of PHI where the 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.
- b. Breach Notification Rule means Subpart D of 45 C.F.R. Part 164.³
 - c. Business Associate⁴ means, with respect to a covered entity, a person that, other than in the capacity of a member of the workforce of the covered entity:
 - i. Creates, receives, maintains or transmits PHI on behalf of a covered entity or an OHCA for a function or activity regulated under the HIPAA administrative simplification rules, such as claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, or repricing; or
 - ii. Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity, if the service involves the disclosure of PHI.
 - iii. business associate also includes:
 - 1. A health information organization (HIO), e-prescribing gateway or other person that provides data transmission services to a covered entity and requires routine access to PHI;
 - 2. A person that offers a personal health record to individuals on behalf of a covered entity; and
 - 3. A subcontractor of a business associate if (i) the business associate delegates to the subcontractor a function, activity or service that the business associate has agreed to perform for the covered entity or for another business associate and (ii) any of the delegated functions, activities or services involve the creation, receipt, maintenance or transmission of PHI.
 - iv. Business Associate does not include:
 - 1. A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual;
 - 2. A plan sponsor, with respect to disclosures by a group health plan (or by a group health insurance issuer or HMO with respect to a group

³ 45 C.F.R. §164.400 – 164.414.

⁴ 45 C.F.R. §160.103.

health plan) to the plan sponsor, to the extent that the requirements of 45 C.F.R. §164.504(f) apply and are met;

3. A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collective PHI for such purposes, to the extent such activities are authorized by law; or
 4. A covered entity participating in an OHCA that performs a function or activity described in subsection (i) of this definition of business associate for or on behalf of the OHCA, or that provides a service described in subsection (ii) of this definition of business associate to or for the OHCA by virtue of such activities or services.
- d. Business Associate Agreement or BAA means a written agreement that satisfies the requirements set forth in 45 C.F.R. § 164.314(a) and 45 C.F.R. § 164.504(e) entered into between a covered entity and a business associate, or between an upstream business associate its downstream subcontractor. A business associate agreement sets forth terms for the business associate’s allowed uses and disclosures of PHI as well as obligations of the business associate with regard to PHI and how PHI will be handled upon termination of the BAA. A BAA is sometimes given titles such as Business Associate Agreement, Business Associate Addendum or Business Associate Contract, or can be reflected in similar provisions within a larger document, such as a contract.
- e. Covered Entity⁵ means a (i) health care provider who transmits any health information in electronic form in connection with a transaction covered under Title 45, Subchapter C of the Code of Federal Regulations (e.g., electronic billing), (ii) a health plan or (iii) a health care clearinghouse.
- f. Downstream Subcontractor⁶ means a subcontractor to whom a business associate delegates a function, activity, or service involving the use or disclosure of PHI, other than in the capacity of a member of the workforce of the business associate.
- g. Electronic Media⁷ means: (i) electronic storage media on which data is or may be recorded electronically including, without limitation, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; (ii) transmission media used to exchange information already in electronic storage media, including, without limitation, the Internet, extranet, or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage

⁵ 45 C.F.R. § 160.103.

⁶ 45 C.F.R. § 164.103, definitions of “subcontractor” and “business associate.” “Downstream business associate” is not a defined HIPAA term, but is sometimes used to distinguish between an upstream business associate and the subcontractor to which it delegates some of its responsibilities.

⁷ 45 C.F.R. §160.103.

- media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.
- h. Electronic PHI⁸ or ePHI means PHI that is transmitted by electronic media or maintained in electronic media.
 - i. HIPAA means the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996, as amended.
 - j. HIPAA Rules means the Privacy, Security, Breach Notification and Enforcement Rules codified at 45 C.F.R. Parts 160 and 164.
 - k. HITECH Act means the Health Information Technology for Economic and Clinical Health Act (Title XIII, Subtitle D).
 - l. Individually Identifiable Health Information⁹ means information, including demographic information collected from an individual, that (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; (2) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual; and (3) either identifies the individual or with respect to which there is a reasonable basis to believe the Information can be used to identify the individual.
 - m. NIST means the National Institute for Standards and Technology.
 - n. OCR means the Office for Civil Rights, which is an agency within HHS that implements, interprets and enforces the HIPAA Rules.
 - o. OHCA or Organized Health Care Arrangement means an “organized health care arrangement” as defined at 45 C.F.R. §160.103. In general, an OHCA is an arrangement among separate covered entities participating in joint activities that involve the sharing of PHI, such as a hospital and physicians on its medical staff.
 - p. Omnibus Rule means the amendments to the HIPAA Rules, published in the Federal Register on January 25, 2013, with a compliance date of September 23, 2013.
 - q. Protected Health Information¹⁰ or PHI means individually identifiable information transmitted or maintained in any form or medium, excluding information in education records covered by the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g, in records described at 20 U.S.C. 1232g(a)(4)(B)(iv), in employment records held by

⁸ 45 C.F.R. §160.103.

⁹ 45 C.F.R. § 160.103.

¹⁰ 45 C.F.R. § 160.103.

a covered entity in its role as employer, and information regarding a person who has been deceased for more than 50 years.

- r. Physical Safeguards¹¹ means physical measures, policies, and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.
- s. Privacy Rule means the Standards for the Privacy of Individually Identifiable Information set forth in Subpart E of 45 C.F.R. Part 164.¹²
- t. Security Rule means the Security Standards for the Protection of Electronic Protected Health Information set forth in Subpart C of 45 C.F.R. Part 164.¹³
- u. Subcontractor¹⁴ means a person to whom a business associate delegates a function, activity, or service that the business associate has agreed to perform for a covered entity or business associate, other than in the capacity of a member of the workforce of such business associate. A subcontractor is considered a business associate where such a delegated function activity, or service involves the creation, receipt, maintenance, or transmission of protected health information.
- v. Technical Safeguards¹⁵ means the technology and the policies and procedures for its use that protect ePHI and control access to it.
- w. Unsecured PHI¹⁶ means PHI that has not been rendered unusable, unreadable or indecipherable to unauthorized persons through the use of a technology or methodology specified by the HHS Secretary in guidance published by the HHS Secretary under the HITECH Act. Such guidance is set forth in Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals, available at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html> and provides that PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals (and is therefore not unsecured PHI) only if either of the following applies:
 - i. ePHI has been encrypted by the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key in accordance with the NIST standards referenced in the guidance and the confidential process or key that might enable decryption has not been breached; or

¹¹ 45 C.F.R. § 164.304 and 164.310.

¹² 45 C.F.R. §164.500 – 164.534.

¹³ 45 C.F.R. §164.302 – 164.318.

¹⁴ 45 C.F.R. § 160.103; 78 Fed. Reg. 5565, 5574 (January 25, 2013).

¹⁵ 45 C.F.R. § 164.304 and 164.312.

¹⁶ 45 C.F.R. § 164.402.

- ii. the media on which the PHI is stored or recorded has been destroyed in one of the following ways: (i) shredding or destruction (in the case of paper, film or other hard copy media), such that the PHI cannot be read or otherwise cannot be reconstructed, or (ii) clearing, purging or destruction of electronic media consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.
- x. Upstream Business Associate¹⁷ means a business associate that delegates a function, activity, or service to a subcontractor involving the use or disclosure of PHI.
- y. Workforce¹⁸ means, with respect to a covered entity or business associate, employees, volunteers, trainees and other persons whose conduct, in the performance of work for such covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

2. HIPAA Background.

- a. HIPAA Rules (45 C.F.R. Parts 160 and 164):
 - i. General administrative provisions, definitions and the Enforcement Rule
 - ii. Privacy Rule: protects the privacy of protected health information (PHI) and sets forth patient rights with regard to the use and disclosure of PHI
 - iii. Security Rule: requires covered entities and business associates to implement reasonable and appropriate administrative, physical and technical safeguards to:
 - 1. ensure the confidentiality, integrity and availability of ePHI;
 - 2. protect against reasonably foreseeable threats or hazards to the security or integrity of ePHI; and
 - 3. ensure workforce compliance with the Security Rule
 - iv. Breach Notification Rule: requires business associates to notify covered entities and covered entities to notify individuals (and report to HHS and, in some cases, the press) upon discovering a breach of unsecured PHI.
- b. The HIPAA Rules apply primarily to two categories of individuals and organizations, namely, covered entities and business associates.

¹⁷ “Upstream business associate” is not a defined HIPAA term but is sometimes used to distinguish between a business associate and its subcontractor.

¹⁸ 45 C.F.R. § 160.103.

- i. In general, any individual (other than a member of the covered entity's or business associate's workforce) or organization that performs or furnishes any function, activity or service for or on behalf of a covered entity involving the use or disclosure of PHI is deemed to be a business associate. See section 1 definition of business associate.
- c. The Privacy and Security Rules allow covered entities to disclose PHI to business associates, and allow business associates to create and receive PHI on behalf of the covered entity, subject to the terms of a business associate agreement between the parties.
- d. Historically, business associates were contractually required to maintain the privacy and protect the security of PHI as provided in their business associate agreements (that is, if they entered into a business associate agreement), but were not subject to sanctions under the HIPAA rules for noncompliance with their business associate agreements or HIPAA Rules.

3. HITECH Act and Omnibus Rule

- a. The obligations and potential exposure of business associates have expanded since the enactment of the HITECH Act and the implementation of the Omnibus Rule.
- b. On February 17, 2009, President Obama signed into law the American Recovery and Reinvestment Act of 2009, including the Health Information Technology for Economic and Clinical Health Act (known as the "HITECH Act" or "HITECH").
 - i. The HITECH Act expanded the HIPAA obligations and exposure of business associates by:
 - 1. applying many of the HIPAA rules directly to business associates;
 - 2. requiring business associates to comply with breach notification requirements;
 - 3. subjecting business associates to civil and criminal penalties for HIPAA violations; and
 - 4. increasing HIPAA enforcement activities and penalties.
- c. The Omnibus Rule amended the Privacy, Security, Breach Notification and Enforcement Rules to implement various HITECH provisions. Significant changes relating to business associates include the following (some of which went beyond the provisions of the HITECH Act):
 - i. Apply the Security Rule and a number of Privacy Rule obligations directly to business associates;

- ii. Extend the business associate definitions and related HIPAA obligations to new categories of business associates, including companies that store or transmit PHI and subcontractors of business associates;
 - iii. Require the amendment of business associate agreements to incorporate the new standards;
 - iv. Expand the potential liability of covered entities to include exposure for the acts and omissions of a business associate if the business associate is deemed to be an agent of the covered entity and the acts or omissions are within the scope of the agency; and
 - v. Subject business associates to potential liability for the acts and omissions of their subcontractors who are deemed to be agents of the business associate.
- d. Covered entities and business associates have been required to comply with the Omnibus Rule since September 23, 2013.
- e. Anyone who performs services or functions that fit within the definition of business associate will be subject to the business associate obligations under the HIPAA rules, even if no business associate agreement is signed.
- f. Business associates now have an obligation to identify their business associate relationships and satisfy the HIPAA rules in connection with those relationships.
- g. Expansion of business associate definition to encompass subcontractors:
 - i. Anyone, other than a member of a covered entity's or business associate's workforce, who assists a business associate in performing a function, activity or service that the business associate has agreed to perform for a covered entity is potentially subject to the HIPAA rules as a subcontractor business associate if the function, activity or services involves access to PHI.
 - ii. HIPAA obligations and potential liability can now extend to subcontractors who have no direct connection or relationship with any covered entity, no matter how far the PHI flows down the chain from business associate to subcontractors and how little the subcontractor knows about the relationship with the covered entity. For example:
 - 1. If business associate A engages subcontractor B to perform part of business associate A's responsibilities involving the covered entity's PHI, subcontractor B in turn delegates some of its responsibilities involving the PHI to subcontractor C, and subcontractor C delegates part of its responsibilities to subcontractor D, then subcontractors B, C and D (as well as business associate A) would all be considered

business associates of the covered entity and the HIPAA business associate obligations would extend down the chain from business associate A to subcontractors B, C and D.

2. In addition, business associate agreements would be required between:
(1) the covered entity and business associate A, (2) business associate A and subcontractor B, (3) subcontractor B and subcontractor C and (4) subcontractor C and subcontractor D.

4. When is a Law Firm a Business Associate?

- a. A law firm will typically be a business associate if:
 - i. The law firm is engaged by a covered entity (e.g., health care provider or health plan) to provide legal services; and
 - ii. The law firm obtains access to the covered entity's PHI in connection with the representation.
 1. Consider whether PHI is needed.
- b. Examples of engagements that may create business associate relationships include (if access to PHI):
 - i. Malpractice defense
 - ii. Payor (reimbursement) audits and disputes
 - iii. Internal investigations
 - iv. Responding to patient service complaints
 - v. Disciplinary actions (licensing, medical staff privileges)
 - vi. Responding to nonparty subpoenas and similar requests for medical records
 - vii. Collection
 - viii. Breach notification and response
- c. Law firm as subcontractor business associate:
 - i. A law firm that is engaged by a business associate in connection with the business associate's responsibilities to a covered entity may be deemed a business associate if the engagement involves access to PHI.
 1. Example: a law firm business associate may retain a second law firm to provide assistance in representing a covered entity on issues involving access to PHI, in which case the second law firm may be a subcontractor business associate.
 - ii. If a law firm is retained for purposes of a business associate's (and not a covered entity's) management and administration, the law firm would likely

not be considered a subcontractor business associate, although the right of a business associate to use or disclose PHI for its management and administration would be dependent on including this right within the business associate's BAA with the covered entity.

1. The preamble to the Omnibus Rule notes that a business associate's disclosure of PHI for its (and not the covered entity's) management and administration would not create a subcontractor business associate relationship, although the Privacy Rule would still require (a) reasonable assurances that the PHI will be held confidentially and will not be disclosed except as required by law or for the purposes of the disclosure, and (b) agreement by the recipient of the PHI (in this case, the law firm) to notify the business associate if the recipient of the PHI becomes aware that confidentiality of the PHI has been breached.¹⁹

5. HIPAA Obligations of Lawyer Business Associates. Some of the principal HIPAA obligations of lawyer business associates are noted below.

a. Business Associate Agreement (BAA).

- i. The Privacy and Security Rules allow a covered entity to disclose PHI to a business associate, and allow a business associate to create, receive, maintain or transmit PHI on the covered entity's behalf, if the covered entity obtains satisfactory written assurances (by entering into a business associate agreement) that the business associate will appropriately safeguard the PHI.²⁰
- ii. Required business associate agreement terms.²¹
 1. The permitted and required uses and disclosures of PHI by the business associate;
 2. No use or disclosure of PHI by the business associate in a manner that would violate the Privacy Rule if done by the covered entity, except that a BAA may permit the business associate to use and disclose PHI for the proper management and administration of the business associate or to carry out the legal responsibilities of the business associate, and may permit a business associate to provide data aggregation services relating to the health care operations of the covered entity (see discussion of optional provisions below);
 3. The BAA must provide that the business associate will:

¹⁹ 78 Fed. Reg. 5565, 5574 (January 25, 2013).

²⁰ 45 C.F.R. § 164.502(e)(1)(i) and (2); 45 C.F.R. § 164.308(b)(1) & (3).

²¹ 45 C.F.R. § 164.314(a) and 45 C.F.R. § 164.504(e).

- a. not use or disclose PHI other than as permitted or required by the BAA, or as required by law;
- b. Use appropriate safeguards to prevent use or disclosure of PHI other than as provided in the BAA;
- c. Comply with the Security Rule;
- d. Report to the covered entity:
 - i. Any known use or disclosure of PHI that is not in accordance with the BAA;
 - ii. Any security incident;²² and
 - iii. Breaches of unsecured PHI as required by the Breach Notification Rule;
- e. Enter into a BAA with any subcontractors that receive, maintain or transmit PHI on behalf of the BA, including the agreement of the subcontractor to the same restrictions and conditions that apply to the business associate;²³
- f. Make PHI available in order to comply with the business associate's obligations to provide individuals with access to PHI and amend PHI in the unlikely event that the lawyer business associate maintains PHI in designated record sets,²⁴ and to provide an accounting of disclosures;
- g. To the extent the business associate carries out a covered entity's obligation under the Privacy Rule, the business associate must comply with the requirements of the Privacy Rule that apply to the covered entity;
- h. Make its internal practices, books and records relating to the use and disclosure of the covered entity's PHI available to the HHS Secretary for purposes of determining the covered entity's compliance with the Privacy Rule; and
- i. At the termination of the BAA, the business associate must:

²² A security incident is an attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

²³ This requirement that any subcontractor agree to terms at least as stringent as those in the BAA between the covered entity and the direct business associate may create challenges for business associates that engage subcontractors.

²⁴ A designated record set is a group of the following records maintained by or for a covered entity: (i) records and billing records about individuals maintained by or for a covered health care provider; (ii) the enrollment, payment, claims adjudications, and case or medical management record systems maintained by or for a health plan; or (iii) a group of records used, in whole or in part, by or for the covered entity to make decisions about individuals.

- i. If feasible, return or destroy all PHI received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains, and retain no copies of such information; or
 - ii. If return or destruction is not feasible, extend the protections of the BAA to the PHI and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible.
- j. The BAA must allow the covered entity to terminate the BAA if the covered entity determines that the business associate has violated a material term of the BAA.
- iii. OCR has posted sample business associate agreement provisions at <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html>. These provisions are generic (and not specific to lawyers) but may be helpful in preparing BAAs.
- iv. If only a limited data set is disclosed to a business associate, then in some cases the covered entity and business associate may enter into a data use agreement, in lieu of a BAA. The required elements of a data set agreement is somewhat less stringent than a BAA.²⁵
- v. In addition to the mandatory terms listed above, a covered entity and business associate (or a business associate and its downstream subcontractor) are allowed to include other provisions within their business associate agreements, or to set forth more stringent standards than required. Some of the issues that are commonly addressed include:
 - 1. A BAA may permit the business associate to use and disclose PHI for the proper management and administration of the business associate or to carry out the legal responsibilities of the business associate, and may permit a business associate to provide data aggregation services relating to the health care operations of the covered entity.²⁶
 - a. The business associate's right to use and disclose PHI for its management and administration is dependent on the business associate agreement.
 - b. With respect to disclosure for the business associate's management and administration, or to carry out its legal responsibilities, the disclosure must satisfy one of the following: the disclosure is required by law; or the business

²⁵ See 45 C.F.R. § 164.514(e).

²⁶ 45 C.F.R. § 164.504(e)(4).

associate must obtain reasonable assurances from the recipient that the PHI will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed. In addition, the recipient must notify the business associate upon becoming aware of any breach of the confidentiality of the PHI.

2. Insurance and indemnification obligations;
 3. Business associate breach notification deadlines and obligations that may be more demanding than those set forth in the Breach Notification Rule;
 4. Notice and cure periods; and
 5. Restrictions on the ability of a business associate to delegate its responsibilities to subcontractors.
- vi. Existing business associate agreements are required to be amended in order to comply with the Omnibus Rule, although transition provisions allow covered entities and business associates to continue to operate under existing business associate agreements for up to one year beyond the compliance date (until September 22, 2014) if the business associate agreement: (1) is in writing, (2) was in place prior to January 25, 2013 (the publication date of the Omnibus Rule), (3) complies with the Privacy and Security Rules as in effect immediately prior to January 25, 2013, and (4) is not modified or renewed.²⁷

b. Business Associate Agreements - Subcontractors.

- i. The HIPAA Rules allow a business associate (an upstream business associate) to disclose PHI to a downstream subcontractor, and allow a subcontractor to create, receive, maintain or transmit PHI on the upstream business associate's behalf, if the upstream business associate obtains satisfactory written assurances (in the form of a business associate agreement) that the subcontractor will appropriately safeguard the PHI.²⁸
- ii. With respect to subcontractors, the upstream business associate (and not the covered entity) with the direct relationship to the downstream subcontractor is responsible for entering into the BAA with the subcontractor.²⁹
- iii. If a law firm is a subcontractor business associate, the law firm and the upstream business associate will be required to enter into a BAA.

²⁷ See 45 C.F.R. § 164.532.

²⁸ 45 C.F.R. § 164.502(e)(1)(ii) and (2); 45 C.F.R. § 164.308(b)(2) & (3).

²⁹ 45 C.F.R. § 164.502(e)(1)(i); 45 C.F.R. § 164.308(b)(1).

- iv. If a law firm engages a subcontractor to perform some of the law firm's functions for a covered entity involving PHI, the law firm will be considered an upstream business associate and will be required to enter into a BAA with its subcontractor.
 - 1. The preamble to the Omnibus Rule expresses OCR's view that a document disposal firm engaged by a business associate to dispose of documents that include PHI would be considered a subcontractor of the business associate, but would not be a subcontractor if it disposes only of documents that do not include PHI.³⁰
- v. In 2005, HHS stated as follows in an FAQ relating to the obligation of a lawyer business associate to require compliance with the Privacy Rule by those to whom the lawyer discloses PHI:
 - 1. Pursuant to its business associate contract, a lawyer must ensure that other legal counsel, jury experts, document or file managers, investigators, litigation support personnel, or others hired by the lawyer to assist the lawyer in providing legal services to the covered entity, will also safeguard the privacy of the protected health information the lawyer receives to perform its duties. Conversely, a lawyer-business associate need not ensure that opposing counsel, fact witnesses, or other persons who do not perform functions or services that assist the lawyer in performing its services to the client, agree to the business associate restrictions and conditions, even though the lawyer may have to disclose protected health information to these third parties.³¹
- vi. The Omnibus Rule expanded the potential liability of business associates to include exposure for the acts and omissions of a subcontractor if the subcontractor is deemed to be an agent of the business associate under the federal common law of agency³² and the acts or omissions are within the scope of the agency.³³
 - 1. The preamble to the Omnibus Rule identified the right or authority to control the subcontractor's conduct as the essential factor in determining whether an agency relationship exists between an upstream business associate and its subcontractor (or between a covered entity and its business authority).³⁴

³⁰78 Fed. Reg. 5565, 5574 (January 25, 2013).

³¹http://www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/709.html

³²For discussion of federal common law of agency, see *Nationwide Mutual Ins. Co., v Darden*, 503 U.S. 318 (1992), and *Community For Creative Non-Violence v Reid*, 490 U.S. 730 (1989).

³³45 C.F.R. 160.402(c)(2).

³⁴78 Fed. Reg. 5565, 5581-2 (January 25, 2013).

2. The preamble indicated that the authority to give interim instructions or directions is the type of control that distinguishes between agency and non-agency relationships and noted that if the only avenue of control is to amend the terms of an agreement or sue for breach, the subcontractor is not acting as an agent of the business associate.³⁵
 3. A law firm that structures the engagement of outside experts to fit within attorney-client protection may be deemed to have engaged the consultant as a subcontractor and to have created an agency relationship. This traditional approach could therefore expose the law firm to potential agency liability in the event that the expert fails to protect the privacy or security of PHI.
- vii. An upstream business associate that delegates some of its responsibilities to a subcontractor will not be in compliance with its obligations under the HIPAA Rules if the business associate knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor's obligations under the BAA between the business associate and the subcontractor, unless the upstream business associate took reasonable steps to cure the breach or end the violation and, if the steps are unsuccessful, terminates the BAA, if feasible.³⁶
- c. Security Rule Obligations of Lawyer Business Associates:
- i. The Security Rule requires covered entities and business associates that use or maintain ePHI to implement administrative, physical and technical safeguards.
 1. For some law firms, implementing these safeguards will present information technology, financial and other challenges.
 - ii. Administrative safeguards are administrative actions, policies, and procedures that manage the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of workforce members in relation to the protection of that ePHI.³⁷ Administrative safeguards include:
 1. risk analysis;
 2. risk management;
 3. regular review of system activity;
 4. security incident procedures;
 5. appointment of a security officer;
 6. workforce sanction policy;
 7. workforce security;
 8. training; and

³⁵ Id.

³⁶ 45 C.F.R. § 164.504(e)(1)(iii).

³⁷ See 45 C.F.R. §§ 164.304 and 164.310

9. contingency plans.
- iii. Physical safeguards are physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.³⁸ Physical safeguards include:
 1. facility access controls;
 2. workstation use;
 3. security controls;
 4. device controls; and
 5. media controls.
 - iv. Technical Safeguards are the technology and the policy and procedures for its use that protect ePHI and control access to it.³⁹ Technical safeguards include:
 1. access controls;
 2. audit controls;
 3. integrity controls;
 4. user authentication controls; and
 5. transmission security.
 - v. The Security Rule designates some safeguards as required and others as addressable.⁴⁰
 1. If a security implementation specification is required, the covered entity or business associate must implement the specification as the Security Rule provides.
 2. If a security implementation specification is addressable, the covered entity or business associate may consider the implementation specification against other alternatives based upon the size, complexity, and capability of the organization. It is important to keep in mind, however, that addressable security implementation specifications are not optional. With respect to an addressable specification, the covered entity or business associate must:
 - a. Assess whether the implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting ePHI; and
 - b. Implement the specification if reasonable and appropriate or, if implementing the specification is not reasonable and appropriate:

³⁸ See 45 C.F.R. §§ 164.304 and 164.310

³⁹ See 45 C.F.R. §§ 164.304 and 164.312

⁴⁰ See 45 C.F.R. § 164.306(d).

- i. Document why it would not be reasonable and appropriate to implement the specification; and
 - ii. Implement an equivalent alternative measure that is reasonable and appropriate and would accomplish the same purpose.
- d. Other business associate Privacy Rule obligations include:
 - i. Use and disclose PHI only as permitted or required by its BAA, or as required by law;⁴¹
 - ii. Prohibition on the “sale” of PHI without the individual’s written authorization;⁴²
 - iii. When using or disclosing PHI, or requesting PHI from a covered entity or business associate, a business associate must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose, unless an exception to the minimum necessary restriction applies.⁴³
- e. HHS Access to Records.
 - i. The HIPAA Rules require business associates to disclose PHI to the HHS Secretary and cooperate when requested in connection with investigations to determine the business associate’s or covered entity’s compliance.⁴⁴
- f. Breach Notification.
 - i. The Breach Notification Rule sets forth a chain of reporting obligations when a breach of unsecured PHI is discovered.
 - 1. If a business associate discovers a breach of unsecured PHI, the business associate is required to notify the covered entity of the breach (or the upstream business associate, if the business associate that discovers the breach is a subcontractor) without unreasonable delay, and in no event more than 60 days after discovery of the breach.⁴⁵

⁴¹ 45 C.F.R. § 164.502(a)(3).

⁴² 45 C.F.R. § 164.502(a)(5)(ii). Sale is generally defined as a disclosure of PHI in exchange for direct or indirect remuneration (financial or otherwise) from or on behalf of the recipient.

⁴³ 45 C.F.R. § 164.502(b).

⁴⁴ 45 C.F.R. § 160.310 and 164.502(a)(4)(i).

⁴⁵ 45 C.F.R. § 164.410.

2. The covered entity is required to notify individuals and HHS (and the media, if the breach involves more than 500 residents of any state) upon discovery of a breach of unsecured PHI.⁴⁶
 - ii. The Omnibus Rule revised the standard under the Breach Notification Rule for determining whether a breach occurred and therefore triggers breach notification obligations.
 1. Under this new standard, an acquisition, access, use or disclosure of unsecured PHI that is not permitted under the Privacy Rule is presumed to be a breach unless either the incident satisfies one of three relatively narrow exceptions, or the covered entity or business associate demonstrates a low probability that PHI has been compromised.⁴⁷ This determination is now based on a risk assessment of at least the following four factors: (1) the nature and extent of the PHI, including the types of identifiers and the likelihood of re-identification; (2) the unauthorized person who used or accessed the PHI; (3) whether the PHI was actually acquired or viewed; and (4) the extent to which the risk is mitigated (for example, by obtaining reliable assurances by recipients of PHI that the information will be destroyed or will not be used or disclosed).
 - iii. With respect to the deadline for breach notification, a breach is deemed to be discovered by a business associate when the breach is first known to the business associate, or would have been known to the business associate had the business associate exercised reasonable diligence.⁴⁸
 - iv. Even if PHI is lost or stolen, the notification obligations under the Breach Notification Rule could be avoided if the information is encrypted (in accordance with NIST standards) or destroyed.
6. Interplay of HIPAA and the Illinois Rules of Professional Conduct (RPC). RPC provisions that warrant particular attention for lawyer business associates include the following:
 - a. The obligation to enter into a business associate agreement, as well as ongoing representation on matters affected by the business associate relationship, need to be considered in light of RPC 1.8 (conflict of interest - transactions), RPC 1.7 and RPC 1.4 (communication).
 - i. RPC 1.8 requirements for lawyer business transactions with clients include:

⁴⁶ 45 C.F.R. § 164.404.

⁴⁷ 45 C.F.R. § 164.402.

⁴⁸ 45 C.F.R. § 164.410(a)(2).

1. Terms must be “fair and reasonable to the client and are fully disclosed and transmitted in writing in a manner that can be reasonably understood by the client;”
2. Client is informed in writing that the client may seek the advice of independent counsel and is given the opportunity to do so;
3. Client gives written informed consent⁴⁹ to the essential terms, and the lawyer’s role; and
4. Lawyer shall not use information relating to representation of a client to the disadvantage of the client unless the client gives informed consent.

ii. Comment 3 to RPC 1.8:

1. “The risk to a client is greatest when the client expects the lawyer to represent the client in the transaction itself or when the lawyer’s financial interest otherwise poses a significant risk that the lawyer’s representation of the client will be materially limited by the lawyer’s financial interest in the transaction. Here the lawyer’s role requires that the lawyer must comply, not only with the requirements of paragraph (a), but also with the requirements of Rule 1.7. Under that Rule, the lawyer must disclose the risks associated with the lawyer’s dual role as both legal adviser and participant in the transaction, such as the risk that the lawyer will structure the transaction or give legal advice in a way that favors the lawyer’s interests at the expense of the client. Moreover, the lawyer must obtain the client’s informed consent. In some cases, the lawyer’s interest may be such that Rule 1.7 will preclude the lawyer from seeking the client’s consent to the transaction.”

iii. RPC 1.4(b) requires a lawyer to explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

b. HHS access to records creates potential concerns with regard to an attorney’s confidentiality obligations under RPC 1.6.

- i. RPC 1.6(a) prohibits a lawyer from revealing information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation, or the disclosure is permitted by RPC 1.6(b) or (c).

⁴⁹ See definition of “informed consent” in RPC 1.0(e) and related discussion in Comments 6 and 7 to RPC 1.0.

- ii. RPC 1.6(b)(6) allows a lawyer to reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary to comply with other law or a court order.
- iii. Comments 12 and 13 to RPC 1.6 address disclosures required by law:
 - 1. “[12] Other law may require that a lawyer disclose information about a client. Whether such a law supersedes Rule 1.6 is a question of law beyond the scope of these Rules. When disclosure of information relating to the representation appears to be required by other law, the lawyer must discuss the matter with the client to the extent required by Rule 1.4. If, however, the other law supersedes this Rule and requires disclosure, paragraph (b)(6) permits the lawyer to make such disclosures as are necessary to comply with the law.”
 - 2. “[13] A lawyer may be ordered to reveal information relating to the representation of a client by a court or by another tribunal or governmental entity claiming authority pursuant to other law to compel the disclosure. Absent informed consent of the client to do otherwise, the lawyer should assert on behalf of the client all nonfrivolous claims that the order is not authorized by other law or that the information sought is protected against disclosure by the attorney-client privilege or other applicable law. In the event of an adverse ruling, the lawyer must consult with the client about the possibility of appeal to the extent required by Rule 1.4. Unless review is sought, however, paragraph (b)(6) permits the lawyer to comply with the court’s order.”
- iv. HHS has stated in its 2002 commentary to the Privacy Rule that: “The Privacy Rule is not intended to interfere with attorney-client privilege. Nor does the Department anticipate that it will be necessary for the Secretary to have access to privileged material in order to resolve a complaint or investigate a violation of the Privacy Rule. However, the Department does not believe that it is appropriate to exempt attorneys from the business associate requirements.”⁵⁰
- v. RPC 1.4(a) requires a lawyer to promptly inform the client of any decision or circumstance with respect to which the client’s informed consent is required under the RPC.
- c. RPC 5.1 and 5.3 (supervision of personnel) overlaps with HIPAA requirements for training and for subcontractor relationships
 - i. RPC 5.3 requires law firm partners and managers to make reasonable efforts to ensure that the firm implements measures giving reasonable assurance that

⁵⁰ 67 Fed. Reg. 53181, 53253 (August 14, 2002).

the conduct of persons employed, retained by or associated with the firm is compatible with the professional obligations of the lawyer

- d. Comments 16 and 17 to RPC 1.6 acknowledge that lawyers have obligations to implement safeguards against inadvertent or unauthorized disclosure.
- e. Obligation to return or destroy PHI upon termination.
 - i. In the 2002 preamble to the Privacy Rule, HHS noted that some commenters expressed concern that the requirement that a lawyer business associate return or destroy PHI at the termination of the BAA is inconsistent with obligations of lawyers. HHS responded that:
 - 1. “With respect to the requirement for the return or destruction of protected health information, the Rule requires the return or destruction of all protected health information at termination of the contract only where feasible or permitted by law. Where such action is not feasible, the contract must state that the information will remain protected after the contract ends for as long as the information is maintained by the business associate, and that further uses and disclosures of the information will be limited to those purposes that make the return or destruction infeasible.”⁵¹

⁵¹ 67 Fed. Reg. 53181, 53253 (August 14, 2002).