Ethical Pitfalls and Legal Risks for Attorneys as Business Associates Under HIPAA

April 3, 2014

Carol D. Scott, Partner, Los Angeles, California

Introduction



Carol D. Scott, Partner, Hinshaw & Culbertson LLP
Los Angeles Office
Phone: 310-909-8015 | **Email:** cscott@hinshawlaw.com

Carol Scott is a partner in Hinshaw's Los Angeles office and a member of the Health Care Practice Group. She advises clients on business, regulatory, corporate and compliance issues, including structuring public-private partnerships and provider alliances; privatization of public systems; contracts, leasing, purchase and sale transactions; licensing, credentialing, certification and accreditation; Medicare and Medicaid audits and third-party billing disputes; billing and reimbursement issues; fraud and abuse, self-referral and anti-kickback issues; antitrust; risk management; HIPAA privacy and security; as well as compliance and bioethics for a broad range of health care providers. Carol earned her B.A. from the University of California at Los Angeles, her M.P.H. from Harvard School of Public Health, and her J.D. from the University of California at Los Angeles.

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Why talk about this now?

- 1996 Health Insurance Portability and Accountability Act (HIPAA) set minimum federal privacy floor
- February 2009 -Health Information Technology for Economic and Clinical Health Act (the "HITECH Act")
- HITECH created sweeping changes to the HIPAA Privacy and Security rules, and extended the obligations of physicians, hospitals, group health plans and other "covered entities" to protect PHI ("Protected Health Information") to "business associates" (BAs)
- In September, 2013, the final regulations and modifications to the HITECH Act, called the "Omnibus Rule", went into effect.

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Omnibus Rule

- The Omnibus Rule includes stiffer penalties for privacy and security violations, increases patient rights, limits use of PHI for marketing, mandates breach notification and most importantly -- creates new requirements for all BAs –including attorneys.



© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

The Omnibus Rule includes

- Direct liability for BAs under HIPAA
- New enhanced enforcement provisions and higher fines
- Increased government audit activities
- Requirements for BA workforce training
- Requirements for BA internal audits and risk analysis and assessments
- Requirements for BA breach notification

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Are you a Business Associate ("BA")?

- **Business Associate**: A person who is not a member of a Covered Entity ("CE")'s workforce who: (i) creates, receives, maintains, or transmits Protected Health Information ("PHI"); or (ii) performs functions or activities on behalf of, or provides certain services (including legal services), for a CE that involve the use/disclosure of PHI from the CE-- or from another BA of a CE.
- **Covered Entity:** (1) health plans, (2) healthcare clearinghouses, and (3) healthcare providers (hospitals, doctors, clinics) that conduct certain transactions (e.g. billing) in an electronic form.
- **Workforce**: employees, volunteers, trainees or others whose work for a CE or BA is under the direct control of the CE or BA, whether or not they are paid.



© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Who is A BA?

- Attorneys may be BAs because they receive or transmit PHI in the course of representing a CE or a BA
- If you are a BA, any vendors or consultants to whom you transmit PHI or who maintain PHI for your CE or BA client are BAs as well (e.g., expert witnesses, court reporters, mediators, accountants, actuarials, shredding companies, etc.)
- Subcontractors of BAs that create, receive, maintain or transmit PHI on behalf of the BA are BAs, whether or not there is a written contract between the attorney and the subcontractor.

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Are you a BA?

Do you represent a BA or a CE? *and*

In the course of the representation do you transmit, maintain, or have access to Protected Health Information ("PHI")?

PHI includes:

Demographic information (name, address, phone, fax, birth month and date, email, social security number), vehicle ID, full face photo, medical history, diagnosis test and laboratory results, insurance information, billing information.

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

When Is An Attorney not a BA?

- Attorneys who receive PHI from individuals or entities who are not a CE or a BA are not BAs

  Examples:

  - Patient gives you his or her PHI
  - Family in conservatorship gives you conservatee's PHI
  - Plaintiff in malpractice case gives you her PHI
  - Workers compensation cases

BEWARE: Even if you are not a BA and HIPAA does not apply, California has strict confidentiality requirements for medical and other confidential information.

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Subcontractors as BAs

- If you are a BA, your vendors and contractors who have access to PHI from you are BAs
- Issue is function not written contract
- HIPAA protects PHI no matter how "far down the chain"
- Can be more than one "layer" of subcontractors --A subcontractor can have a subcontractor who is a BA

Examples:

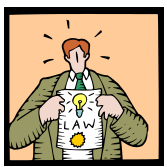
- Law firm retains consultant, expert witness or investigator to assist with representation of CE and he/she reviews PHI
- Law firm uses shredding company to dispose of client files containing PHI



© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

So You are a BA -- What Now?

- You need Business Associate Agreements ("BAAs") with clients who are CEs or BAs
- You need BAAs with consultants, expert witnesses and other subcontractors who have access to, transmit, or use PHI
- Agency liability for the acts of your BAs
- Breach notification obligations under HIPAA (Note, California has breach notification requirements as well)
- Responsibility for compliance with certain Privacy Rule provisions and Security Rule
- Administrative, physical, and technical safeguards for ePHI
- Civil and criminal liability for HIPAA violations



© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

What provisions should be in your BAAs?

- BA must comply with the Security Rule
- BA must report non-permitted uses, breaches of unsecured PHI to CE (to you for reporting)
- BA must ensure any subcontractors that create/receive PHI on behalf of the BA agree to the same restrictions/conditions as the BA
- Agreement should directly reference the Security Rule, not just the Privacy Rule (rather than general reference to safeguards to prevent unauthorized use/disclosure)
- Make sure breach notification obligations are clear, consistent with internal policies, and permit receiving entity sufficient time to investigate and make required reports
- Address ePHI – consider requiring safeguards that render PHI unusable, unreadable and indecipherable to unauthorized individuals

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

BAAs (cont'd)

- Compliance with requests for access from patients, as applicable
- Amendments to PHI
- Availability of Internal Records
- Mitigation
- Termination Provisions

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

BAAs (cont'd)

- Indemnification provisions
  - If you are drafting BAAs for clients and suggesting that they include indemnification provisions, what happens when they want you to sign a similar agreement?
  - If you include an indemnification provision in your subcontractor BAAs, what happens when the subcontractor will not sign the provision?

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Compliance Deadlines

- Compliance Deadline was September 23, 2013 for all BAAs entered into after 1-25-13
- One year transition period for BAAs that were in existence as of January 25, 2013 when the Omnibus Rule was released:
  - These do not need to be modified until they are amended/renewed in the ordinary course of business, but no later than September 23, 2014



© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Privacy Rule Obligations

Develop and Implement and review policies and procedures that include:

- Compliance with Privacy Rule concerning the use, disclosure and protection of PHI to protect against impermissible uses/disclosures of PHI (whether inadvertent or intentional)
- Breach notification
- Access to ePHI to CE, individual, or individual's designee (as specified in BAA)
- Disclosing PHI to HHS and other agencies for compliance investigations
- Accounting of disclosures
- Any provisions that apply to functions/activities delegated to the BA under the BAA
- The minimum necessary standard.
  - Use and disclosure of PHI must be limited to the minimum necessary to accomplish the intended purpose

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Privacy rule obligations (cont'd)

- Record Keeping
- Not required to have Privacy officer but must have security officer.



© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Privacy Rule Requirements



Fortunately, his training had prepared him to deal with all types of customers.

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Security Rule Compliance



- Designate a Security Official
- Establish and implement risk assessment policies and procedures
- Implement appropriate administrative, physical and technical safeguards to address vulnerabilities identified in assessment.
- Develop and implement policies, procedures and forms addressing security obligations
- Develop strategy to monitor BA/subcontractor compliance

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Security Rule Compliance

- Consider obtaining expert assistance from consultants, IT experts, HIPAA experts.
- Know how information flows into, inside and out of your office. Understand your software and devices.



© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Use/Disclosure of PHI by Attorneys

- Use of PHI in litigation or administrative or judicial hearings:

  a. With the individual's written authorization.

  b. Can use PHI without patient authorization:

  (i) for treatment, payment of health care operations purposes --

  - Defending physician in a collection action
  - Defending physician in malpractice action

  (ii) As required by law (court order/ administrative order)-

  (iii) For a proceeding before a health oversight agency (contested licensing revocation)

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Use or Disclosure of PHI in Litigation

When client is a party to the litigation no authorization required -- considered to be part of CE's operations

a. Still subject to minimum necessary, consider taking out identifiers

b. Consider Protective Order to prohibit further disclosure

When not a party to litigation and no exception applies:

a. HIPAA compliant authorization; or

b. Court order; or

c. Subpoena with reasonable assurances: notice, time for objection passed and no objection or objections resolved (45 CFR 164.512); or

d. Qualified Protective Order

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Use of PHI in Litigation

Analysis

1. Does HIPAA apply? Was the information created or received by CE?

2. Is there an exception?

3. Do you need to account for the disclosure?

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Steps to take now…

Business Associate Agreements

Make sure you have updated BAAs with your CE and BA clients

Make sure you have updated BAAs with your consultants, court reporters, experts, investigators forensic accountants and others who use or disclose PHI in assisting you in representing clients. They are your BAs.

Make sure your breach notification provisions are consistent with your updated security incident policies

Firm Policies and Procedures

- Privacy Policies
- Security Policies
- Employee training
- Disciplinary policies and procedures



© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Compliance Suggestions

- Develop a committee
  - IT experts
  - Firm management
  - Lawyers familiar with client and business associate relationships and familiar with the Firm's IT structure and flow of PHI and electronic PHI within the Firm
  - Team effort
- Solo practitioners still have HIPAA obligations



© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

More steps…

- Conduct and document a risk analysis:
  - How do you handle PHI, where is it stored, who has access; what privacy and security protections do you have in place; where are the gaps?
- Develop and Implement Privacy and Security Policies and Procedures
- Address identified gaps
- Conduct and document workforce training

Document, Review, Revise, Reinforce



© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Risk Assessment

- Where do you store PHI? Who has access to PHI? Is access limited? How?
- Do you lock office doors? Leave PHI on desks? Leave PHI in hallways or conference rooms accessible to clients and others?
- Who has access to servers? How is access limited?
- What security do you have at workstations? Do you have passwords/User IDs on computers? Ex: CDe%6x#A Do you have a rule against sharing passwords?
- Is File room locked?
- Are Offices locked?



The sticky notes are for security. We keep passwords on sticky notes so they are safe.

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Risk Assessment

- Faxing/emailing: What policies/ restrictions do you have? How do you transmit PHI? Is it encrypted? Do you confirm receipt of faxes? Use cover sheets? Monitor incoming faxes?
- Are computers timed to shut off when not in use for a set time period?
- Do you have anti-virus software? Do you have policies for adding software and hardware to work stations or the network?



© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Risk Assessment

- Do you keep track of who accesses PHI? Do you have a policy on accessing PHI? Can be PHI be taken off site?
- Do attorneys work off site?
- In case of a disaster, what are the procedures for restoration? Protection of PHI does not just include limiting access but means ensuring appropriate access.



© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Risk Assessment

- Mobile devices -- what policies and procedures and safeguards do you have for laptops, phones, tablets, USB drives?
- Do you require that all mobile devices have passwords? Are they encrypted? What is your backup policy? Can devices be wiped remotely if lost?
- When you return a device, copy machine or other equipment do you ensure that there is no PHI on it?
- When someone leaves the Firm, is access restricted? What about mobile devices?



© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Risk Assessment

- What are your procedures for data retrieval in case of an earthquake, flood, power outage?



"Dan, how do you spell CLOUD?"

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Risk Assessment/Risk Management

- Have you conducted training of workforce members who have access to PHI? Do you document training? Is training updated regularly?
- What efforts are you making to enforce the minimum necessary standard?
- Destruction/disposal
  - What are your destruction/disposal policies?
  - Most BAAs require that PHI be returned at the end of project/For attorneys this may create an ethical dilemma concerning obligations for retaining certain documents and information
- Risk Management Plan/ Internal Audits
- Cyber-insurance

Are you ready for an audit?



© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

HIPAA Breach Notification

- Do you have a breach notification policy?
- Do members of the firm know how to identify a breach and what to do in event of a breach?

  Example:

  An unencrypted laptop stolen from the trunk of a car would require breach notification, a large fine and adverse publicity for the Firm
- Have you tested your breach policy?
- Time frames for notification?

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Federal Breach Notification

- HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.
- FTC also has breach notification rules for vendors of personal health records and their third party service providers.
- **Breach** defined: acquisition, access, use, or disclosure of unsecured PHI, in a manner not permitted by **HIPAA**, which poses a significant risk of financial, reputational, or other harm to the affected individual.

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Breach defined…

- Four parts to definition:

  (1) PHI is unsecured;

  (2) Unauthorized use, access or disclosure violates the Privacy Rule;

  (3) Significant risk that such access, use or disclosure will cause financial, reputational, or other harm to the patient; and

  (4) No exceptions apply.

If any of these four criteria are not met, the situation is incident, not a breach and notification and reports need not be made to OCR, but BA must document, in the form of a risk assessment, the basis for determining there was no breach.

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Risk Assessments

(1) Individuals involved- Who impermissibly used the PHI or to whom was the PHI impermissibly disclosed?

(2) What type and amount of PHI was involved?

(3) Are there mitigating factors-were immediate steps were taken to mitigate an impermissible use or disclosure?

(4) Was the PHI was returned prior to being used for an improper purpose;

(5) Do any exceptions apply?

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Incidents that are NOT a Breach



1. No unsecured PHI involved

PHI was encrypted or in limited data sets that did not include zip codes and dates of birth

2. No Violation of the Privacy Rule

Incidental disclosure that results from an otherwise permissible use or disclosure

3. No risk of harm to patient

Immediate steps taken to mitigate an impermissible use or disclosure

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Examples – not likely to be a Breach

- PHI sent by facsimile to the wrong number and the Covered Entity immediately receives a confidentiality agreement from the unintended recipient.
- PHI returned prior to being accessed for impermissible purposes. (stolen laptop recovered, and forensic analysis determines unencrypted information not accessed.)
- Information presents minimal risk of harm (patient's name and address in a list of patient that does not indicate type of services)

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Exceptions

Three exceptions to the definition of Breach:

(1) The unintended recipient would not reasonably have been able to retain the information (the information is recovered before it could have been seen).

(2) Unintentional or inadvertent disclosures within a CE or BA (a nurse accidentally opens email that was intended for a different nurse) and the information is not further used or disclosed in an impermissible manner.

(3) Unauthorized disclosure where BA has good faith belief that the unauthorized person to whom PHI disclosed would not reasonably have been able to retain the information (EOBs sent to wrong individual but returned unopened by Post Office).

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Probable Breaches

- Incident involving PHI that is also protected by other state and federal confidentiality laws
  - (PHI could be used to steal an individual's identity such as social security number or credit card information and password; or relates to treatment for HIV/AIDS, sexually transmitted diseases, mental health or substance abuse; or employer could use PHI to discriminate against an employee or applicant such as cancer diagnosis).
- Access to PHI by employee without authorization and no job-related reason to do so (employee checking on the health status of a friend)
- Use or disclosure that involves more than the minimum necessary information.

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Breach Notice Requirements



© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

State Breach Notification

California Breach Law Civil Code 1798.29(e) and 1798.82(f))

- A business must notify any California resident whose unencrypted personal information (including medical information) was acquired, or reasonably believed to have been acquired, by an unauthorized person.
- Any person or business required to issue security breach notification 500+ California residents for a single security breach must provide the breach notification to the AG.

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

California Privacy and Security Laws

General

- Confidentiality of Medical Information Act (Civ.Code 56 et seq.)
- CA Customer Records Act (Civ. Code 1798 et. seq.)
- Patient Access to Health Records Act (Health and Safety Code 123100 et seq.)

Additional Attorney Obligations

- CA Rules of Prof. Conduct 3-100; Civ. Code 6068 (See also ABA Model Rule 1.6 (confidentiality of client information)
- CA Evidence Code 952 (Attorney/Client Privilege)
- CA Ethics Opinion 2010-179 (Duty of confidentiality extends to use of technology and risk of unauthorized disclosure)



© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Enforcement actions

- **Violation:** Laptop taken abroad by physician stolen, contained PHI of 3,500 patients. Entity did not: (i) demonstrate risk analysis of ePHI; (ii) require encryption or equivalent security measures; (iii) adopt policies on the use and removal of portable devices- $1.5 in penalties.
- **Violation:** Laptop containing 23,500 patient records stolen from rental car. State AG sued, alleging: (i) failure to implement HIPAA policies; (ii) failure to conduct effective training; (iii) failure to implement policies on portable media containing ePHI. $2.5 in fines. Company banned from operating in State for two years.
- **Violation:** Medical Group's appointments posted on publicly accessible internet calendar. Group failed to have safeguards to protect ePHI, failed to: implement policies and procedures for safeguarding PHI, train employees, identify a security official and conduct a risk analysis and did not have BAA agreements with service providers. $100,000 in fines.

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

More violations….

- **Violation:** Leased copying machines purchased by CBS reporters contained scanned PHI in copier memory from HMO.
- **Violation**: Patient data from 168,000 L.A. County patients stolen when computers stolen from billing office that contracts with Los Angeles County to provide billing and collection services.

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

- Los Angeles Times 10/21/13….Laptop thefts compromise 729,000 hospital patient files

"Thieves steal two laptops containing patient data from an administration building of San Gabriel Valley-based AHMC Healthcare."



© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Questions



© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.

Carol D. Scott, Partner

Hinshaw & Culbertson LLP

Los Angeles | 310-909-8015

cscott@hinshawlaw.com

www.hinshawlaw.com

© 2014 Hinshaw & Culbertson LLP, an Illinois Limited Liability Partnership. All rights reserved.