Hot Topics in HIPAA

American Health Lawyers Association
Hospitals & Health Systems Law Institute
Orlando, Florida
February 14-15, 2008

Phyllis F. Granade
Carlton Fields, P.A.
Atlanta, Georgia

Robert Q. Wilson
The Bogatin Law Firm, PLC
Memphis, Tennessee

1

Disclaimer

This presentation and handouts are for educational and discussion purposes only – nothing herein is legal advice, warranted in any way, or should be relied on as a complete statement of the law.

2

OCR and CMS Enforcement Recap *(by Phyllis Granade)*

3

HIPAA Privacy News
CMS Enforcement Numbers as of 12/31/07

- *From www.hhs.gov/ocr/privacy/enforcement/numbersglance1207.html*
  - –32,487 total complaints (12% increase in 2007 over 2006)
  - –5,501 now closed, but required change in CE practices
  - –2,609 found no violation
  - –24,288 outside jurisdiction (no CE, etc.)
  - –419 cases referred to DOJ for criminal investigation
  - –215 cases referred to CMS for security rule investigation

4

HIPAA Privacy News
CMS Enforcement Numbers as of 12/31/07

- According to OCR, and as reported by *Health Information Privacy/Security Alert*, the compliance issues most commonly investigated this past year were:
  - Impermissible uses and disclosures of protected health data;
  - Lack of safeguards of protected health data;
  - Lack of patient access to their protected health information;
  - Uses or disclosures of more than the Minimum Necessary protected health information; and
  - Lack of or invalid authorizations for uses and disclosures of protected health information.
- This "most commonly investigated" list does not appear to necessarily represent individuals' complaints
  - CEs with Corporate Integrity Agreements frequently self report, and these reports skew investigation numbers
  - For instance, it seems unlikely that patients would necessarily recognize a violation of the minimum necessary standard

5

OCR Enforcement – Official Practices

- Compliance and Enforcement website: www.hhs.gov/ocr/privacy/enforcement
  - Complaint process flowchart (est. 4-20-07)
  - How OCR enforces the rule
    - Voluntary compliance/corrective action
    - Resolution Agreement/Appeal of CMPs
  - OCR looks at complaints to determine:
    - Post 4-14-2003?
    - Activity alleged is violation?
    - CE involved?
    - Filed w/in 180 days (or waiver)?
    - Identity of complainant and consent given to OCR to disclose to CE, subject of PHI, and CE provided
  - OCR complaint investigation flowchart in handouts

6

*Un*official OCR Practices

- Problems with some regional OCR investigators:
  - HIPAA comprehension concerns
  - Overly broad and/or repetitive demands
    - Comment from investigator who received the large volume of documents she requested after she was warned of the size of the request: "You think I'm going to read all of this?"
  - Can take months (or years!) for investigations to begin, and even longer to close
    - '03 complaint, investigation letter in '05, still open in '08
  - CE guilty until proven innocent
  - Decisions made regarding State privacy law, not HIPAA
  - Region IV Director allegedly told investigators to use "individual judgment" when informing CEs of mitigation activities they should be performing (read: "must do")

7

Practical Guidance for Dealing with OCR

- OCR will ask for these items; consider carefully what you provide:
  - Notes of the Privacy Officer regarding the PO's findings/conclusions
  - EHR audit trails
  - Workforce member and complainant interview notes
  - Correspondence between complainant and CE
  - Proof of sanction enforcement against workforce members
  - Odd requests
    - Investigator asked for a copy of a payroll stub to prove pay deduction against workforce member (i.e., time off without pay)
  - Affidavits from workforce members involved in the activity that allegedly violated HIPAA
- Do not rush to hand over materials or admit fault
  - Prior to handing materials over to OCR or CMS, or having substantive discussions with investigators, in-house or outside legal counsel should clear all materials and conversations

8

Action Plan for Responding to OCR/CMS

- Confirm that the use/disclosure **did** or **did not** occur, and if it did occur, whether it was permitted by HIPAA
- Objectively prepare a response explaining your facts, your analysis under HIPAA, and your conclusions
- Response to OCR should include a description of:
  - CE's acceptance of the complaint (if filed with CE)
  - Summary of CE's investigational efforts and findings
  - Detail CE's enforcement efforts and sanctions
  - Details CE's "wrap up" and response to the complainant
- Remain polite and professional, and always objective
- Act and respond promptly

9

Additional Problems with OCR Investigations

- OCR investigators may request action by the facility that is not required by HIPAA
  - consider whether the requested action is appropriate to your circumstances
    - An OCR Region IV investigator told my client that HIPAA requires CEs to notify patients regarding inappropriate disclosures of the patient's PHI. While it may be appropriate to notify patients of such disclosures, HIPAA does not require notification other than accounting for the disclosure.
- HIPAA does not require notification of violations, ***however:***
  - Identify theft and other mitigation concerns may require notification of individuals that their information has been misused or disclosed
    - See **Section II** of Phyllis Granade's outline – Emerging Standards for Responding to Data Loss and Theft

10

HIPAA Security News - CMS Enforcement

- As of the end of 2007, at least seven hospital systems (other than Piedmont) were undergoing Security Audits
  - Why the cloak of silence?
  - Why is CMS targeting non-profit hospital systems?
- "The Centers for Medicare and Medicaid Services (CMS) will begin on-site reviews of hospitals' compliance with security rules mandated by [HIPAA]." **According to officials, between 10 and 20 hospitals will be reviewed within nine months**, beginning with "hospitals where CMS has received complaints about security practices." **Among the issues CMS will examine are "[r]emote access to data and use of portable storage devices" to store hospital records**. Government Health IT noted that "if the review uncovers major lapses, the agency can fine a hospital or levy other punishments."
  - Reported by Government Health IT (1/17/08, Ferris) and cited by the AHLA in a January 18 email briefing

11

CMS Security Audits: Piedmont Hospital

- From www.computerworld.com and confirmed by my sources, CMS sent a letter to Piedmont requesting the following P&Ps within 10 days:
  1. Establishing and terminating users' access to systems housing electronic patient health information (ePHI).
  2. Emergency access to electronic information systems.
  3. Inactive computer sessions (periods of inactivity).
  4. Recording and examining activity in information systems that contain or use ePHI.
  5. Risk assessments and analyses of relevant information systems that house or process ePHI data.
  6. Employee violations (sanctions).
  7. Electronically transmitting ePHI.
  8. Preventing, detecting, containing and correcting security violations (incident reports).
  9. Regularly reviewing records of information system activity, such as audit logs, access reports and security incident tracking reports.
  10. Creating, documenting and reviewing exception reports or logs. Please provide a list of examples of security violation logging and monitoring.
  11. Monitoring systems and the network, including a listing of all network perimeter devices, i.e. firewalls and routers.

12

CMS Security Audits: The Piedmont Hospital Investigation (contd.)

- Additional Requests by CMS:

1. Provide a list of all information systems that house ePHI data, as well as network diagrams, including all hardware and software that are used to collect, store, process or transmit ePHI.
2. Provide a list of terminated employees.
3. Provide a list of all new hires.
4. Provide a list of encryption mechanisms use for ePHI.
5. Provide a list of authentication methods used to identify users authorized to access ePHI.
6. Provide a list of outsourced individuals and contractors with access to ePHI data, if applicable. Please include a copy of the contract for these individuals.
7. Provide a list of transmission methods used to transmit ePHI over an electronic communications network.
8. Provide organizational charts that include names and titles for the management information system and information system security departments.
9. Provide entity wide security program plans (e.g., System Security Plan).

13

CMS Security Audits: The Piedmont Hospital Investigation (contd.)

10. Please provide a list of all users with access to ePHI data. Please identify each user's access rights and privileges.
11. Please provide a list of systems administrators, backup operators and users.
12. Please include a list of antivirus servers, installed, including their versions.
13. Please provide a list of software used to manage and control access to the Internet.
14. Please provide the antivirus software used for desktop and other devices, including their versions.
15. Please provide a list of users with remote access capabilities.
16. Please provide a list of database security requirements and settings.
17. Please provide a list of all Primary Domain Controllers (PDC) and servers (including Unix, Apple, Linux and Windows). Please identify whether these servers are used for processing, maintaining, updating, and sorting ePHI.
18. Please provide a list of authentication approaches used to verify a person has been authorized for specific access privileges to information and information systems.

14

What (Little) We Know About the Outcome of the Piedmont Hospital Security Audit:

- CMS admitted its personnel did not have the experience/ability to conduct a HIPAA security audit
- CMS requested that the Office of Inspector General conduct the security audit due to the OIG's greater experience with investigations, and the OIG agreed
- CMS/OIG demanded that Piedmont maintain complete silence during the investigation and until such time as the investigation is closed (originally anticipated to occur in November 2007). CMS has intimated that additional confidentiality restrictions may be requested of Piedmont following its receipt of the audit closure letter.
- Recently, CMS contracted with Price Waterhouse Coopers to provide "technical assistance" to CMS regarding HIPAA security audits and investigations. Piedmont hired PWC during its audit, and PWC was paid to assist may hospitals and other covered entities during the compliance ramp-up for HIPAA privacy and security.

15

What (Little) We Know About the Outcome of the Piedmont Hospital Security Audit (contd):

- In December 2007, Piedmont apparently received word regarding the Security Audit closure. Although no word has officially been released by Piedmont or CMS/OIG:
  - Piedmont expected to receive a CMS closure letter in November '07
  - In January 2008, Piedmont posted listings for the following job positions with the AHLA:
    - Compliance Director
    - Compliance Education Coordinator
    - Compliance Auditor

16

Security Standards:

Guidance from

Centers for Medicare & Medicaid Services (CMS)

and

National Institute of Standards and Technology

(NIST)

(by Rob Wilson)

17

WHAT ARE GREATEST CURRENT THREATS?

- **Data Breach or Loss**
  - Computer or Media Theft/Loss
  - Offsite Access Points
  - Browser Exploits
  - Gullible Custodians & Insiders

18

Security: CMS and NIST Guidance

- **CMS** Guidance: Remote Use of and Access to ePHI (January 2007)
  - In response to nationwide rash of laptop, portable media, public workstation, and similar losses and breaches involving ePHI
  - Available with other CMS security guidance documents at:

    http://www.cms.hhs.gov/EducationMaterials/04_SecurityMaterials.asp#TopOfPage

19

Security: CMS and NIST Guidance

- **CMS** Guidance: Remote Use of and Access to ePHI (January 2007)
  - CMS enforces HIPAA Security Standards and may rely upon this guidance in determining whether or not actions of covered entity are reasonable and appropriate for safeguarding confidentiality, integrity, and availability of ePHI
  - Guidance may be given deference in administrative hearings under the HIPAA Enforcement Rule

20

Security: CMS and NIST Guidance

- **CMS** Guidance: Remote Use of and Access to ePHI (January 2007)
  - Meat of this guidance was included in proposed amendments to HIPAA Security Standards, but amendments died in governmental internal approval processes, Fall 2007
  - CMS felt amendments would be unnecessary given flexibility, scalability, and technology neutrality built into initial Security Standards

21

Security: CMS and NIST Guidance

- **CMS** Guidance: Remote Use of and Access to ePHI (January 2007)

  . . . covered entities should be extremely cautious about allowing the offsite use of, or access to, ePHI. There may be situations that warrant such offsite use or access, e.g., when it is clearly determined necessary through the entity's business case(s), and then only where great rigor has been taken to ensure that policies, procedures and workforce training have been effectively deployed, and access is provided consistent with the applicable requirements of the HIPAA Privacy Rule.

  (emphasis added)

22

Security: CMS and NIST Guidance

- **CMS** Guidance: Remote Use of and Access to ePHI
  A covered entity must evaluate its own need for offsite use of, or access to, ePHI, and when deciding which security strategies to use, must consider:
  (i) The size, complexity, and capabilities of the covered entity.
  (ii) The covered entity's technical infrastructure, hardware, and software security capabilities.
  (iii) The costs of security measures.
  (iv) The probability and criticality of potential risks to [ePHI].

23

Security: CMS and NIST Guidance

- **CMS** Guidance: Remote Use of and Access to ePHI

Covered entities should place significant emphasis and attention on their:

- Risk analysis and risk management strategies
- Policies and procedures for safeguarding ePHI
- Security awareness and training on the policies & procedures for safeguarding ePHI

24

Security: CMS and NIST Guidance

- **CMS** Guidance: Remote Use of and Access to ePHI

Risks can be approached in three categories for planning purposes:

- **Accessing** ePHI
- **Storing** ePHI
- **Transmitting** ePHI

25

Security: CMS and NIST Guidance

- **CMS** Guidance: Remote Use of and Access to ePHI

Accessing ePHI risks and mitigation management strategies are outlined in the guidance, e.g.,

- Employees access ePHI when not authorized to do so while working offsite
  - Develop and employ proper clearance procedures and verify training of workforce members prior to granting remote access
  - Establish remote access roles specific to applications and business requirements. Different remote users may require different levels of access based on job function
  - Ensure that the issue of unauthorized access of ePHI is appropriately addressed in the required sanction policy

26

Security: CMS Guidance

Storing ePHI risks and management strategies are outlined in the guidance, e.g.,

- Laptop or other portable device is lost or stolen resulting in potential unauthorized/improper access to or modification of ePHI housed or accessible through the device
  - Identify the types of hardware and electronic media that must be tracked, such as hard drives, magnetic tapes or disks, optical disks or digital memory cards, and security equipment and develop inventory control systems
  - Implement process for maintaining a record of the movements of, and person(s) responsible for or permitted to use, hardware and electronic media containing ePHI
  - Require use of lock-down or other locking mechanisms for unattended laptops

27

Security: CMS Guidance

Storing ePHI risks and management strategies are outlined in the guidance, e.g.,

- Laptop or other portable device lost/stolen (*continued*)
  - Password protect files
  - Password protect all portable or remote devices that store ePHI
  - Require that all portable or remote devices that store ePHI employ encryption technologies of the appropriate strength
  - Develop processes to ensure appropriate security updates are deployed to portable devices such as Smart Phones and PDAs
  - Consider the use of biometrics, such as fingerprint readers, on portable devices

28

Security: CMS Guidance

Transmitting ePHI risks and management strategies are outlined in the guidance, e.g.,

- Data intercepted or modified during transmission
  - Prohibit transmission of ePHI via open networks, such as the Internet, where appropriate
  - Prohibit the use of 3rd party offsite devices or wireless access points (e.g., hotel workstations) for non-secure access to email
  - Use more secure connections for email via SSL and the use of message-level standards such as S/MIME, SET, PEM, PGP, etc.
  - Implement and mandate appropriately strong encryption solutions for transmission of ePHI (e.g. SSL, HTTPS etc.). SSL should be a minimum requirement for all Internet-facing systems which manage ePHI in any form, including corporate web-mail systems

29

Security: NIST Guidance

National Institute of Standards and Technology (NIST)

- **Federal agencies must follow NIST guidelines**
- **Voluntary usage by non-Federal organizations**
- **Security Standards Final Rule references to NIST:**

  "[A]n excellent source of information and guidance on this subject [specifically references security training, other references support a broader application] and is targeted at industry as well as government activities,"

  "While we will not assume the task of certifying software and off the- shelf products. . ., we have noted with interest that other Government agencies such as [NIST] are working towards that end. The health care industry is encouraged to monitor the activity of NIST and provide comments and suggestions when requested"

30

Security: NIST Guidance

NIST Special Publication 800-66 re: Security Rule

- Previous version March 2005
- New version being posted at:

  http://csrc.nist.gov/publications/PubsSPs.html
- See outline for more details on content, but . . .

31

Security: NIST Guidance

Updated NIST SP 800-66 will:

- Update crosswalk to other NIST publications on security topics (e.g., security management process, access controls, security awareness and training, contingency planning, evaluation, device & media controls, transmission security (encryption))
- Discuss the latest threats, vulnerabilities, and exposures, as well as the technologies used to combat them
- Include introduction to HIPAA risk management framework
- Include guidelines on risk assessments and contingency planning
- Discuss special considerations when applying the HIPAA Security Rule
- Discussion of the automation of technical safeguards

32

Security: NIST Guidance

Highlights in SP 800-66

- **Approach to Risk Assessments**: Will now recommend one layer of testing rather than two
- **Contingency Plans**: vs. Disaster Recovery
- **Automation**: Preview of where things are heading, e.g.,
  - Federal Desktop Core Configuration (FDCC)
  - Security Content Automation Protocol (SCAP)

33

Responding to Data Loss and Theft *(by Phyllis Granade)*

34

Responding to Data Loss and Theft

- HIPAA Mitigation Requirements, 45 C.F.R. Section 164.530(f)
  - Account for disclosures due to loss/theft, Section 164.528
  - Review info lost/stolen, consider likelihood of identity theft and harm
- Does state law require notification of individuals in the event of loss/theft?
  - Data breach notification laws exist in over 30 states
- No state law notification requirement? CE still must determine if, based upon the data potentially disclosed, the risks of not notifying the individual outweigh the risks of notification.
  - Risk analysis questions for determining whether to notify patients of loss/theft (absent state law notification requirements)
    - What data was lost or stolen?
    - Will the data embarrass the individual, or cause harm to his/her reputation?
    - What is the likelihood the individual may suffer economic harm, such as identity theft (including medical identity/insurance theft)?
    - Could notification cause the individual greater emotional harm than failure to notify? (e.g., low risk of harm from disclosure, patient's mental state frail)

35

State Data Breach Notification Laws

- Over 30 states have data breach notification laws. See list at AHLA website under the HIT practice group.
- California's notification law, summarized below, includes a private right of action:
  - Law applies to gov't and private business
  - Notice required for unauthorized access to nonpublic "personal information," which includes:
    - First name or initial and last name in combo with one or more of the following:
      - SSN
      - Driver's license or ID card #
      - Account, credit or debit card #, in combo with a PIN or access code
  - Expanded on January 1, 2008 to "medical information" and "health insurance information"
  - INFORMATION ENCRYPTED? NO REQUIREMENT TO NOTIFY!
  - Expedient notice must be provided in writing (or electronically in certain circumstances), although:
    - Substitute forms of notice are possible if large # of people are impacted or the cost of notification is high
    - Substitute notice can include email, website and statewide media

36

The Value of Safeguarding Data

- According to an unofficial survey by the California Department of Consumer Affairs' Office of Privacy Protection, about 53% of all data breaches triggering notification resulted from lost or stolen laptops and other portable devices.
- Thoughts:
  - There is a need to improve the protection of data on portable electronic devices
  - There is a need to improve the protection for the actual devices
  - Encryption, an addressable standard under the Security Standards, is a "safe harbor" under data breach notification laws
  - P&Ps to ensure protection of data/devices (plus rigorous enforcement of P&Ps) are essential
- PURGE your data in accordance with your P&Ps
  - Purging old data limits the amount of data that could be lost/stolen; avoids embarrassment and costs associated with losing 30 year old data.

37

Lost/Stolen Data - HIPAA Security Standards

- My experiences with CE data loss and theft (particularly stolen laptops) leads me to the following conclusions regarding improvements that should be made to CE HIPAA security compliance efforts:
  - Clear P&Ps regarding remote access. See HHS/CMS guidance re: remote access.
  - Comply with P&Ps regarding contingency operations and data backup and storage so that data lost or stolen can be promptly recreated. 45 C.F.R. Sections 164.310(a)(2)(i), 164.310(d)(2)(iv).
  - Stop ignoring the importance of implementing and enforcing P&Ps establishing role-based access (e.g., workforce members have limited access to PHI, and on a need-to-know basis). 45 C.F.R. Sections 164.308(a)(4), 164.310(a)(2)(iii), and 164.312(a).

38

Trends in Responding to Data Loss/Theft

- Even if there is no applicable data breach notification law in a state, CEs are typically deciding to notify impacted individuals of a loss or theft if the elements of a model data breach notification law are met.
- Regarding risk of identity theft, CEs should use the risk analysis questions set forth earlier in this presentation.
- Encryption by CEs, unfortunately, is not commonplace.
- Typical data breach notification:
  - Letter sent via USPS first class mail
  - Additional notice on website, or in local media (e.g., press release)
  - Template letter is set forth in your materials
  - Credit monitoring and insurance often offered
- Beef up your indemnification provisions with your vendors to cover mitigation and notification expenses

39

Application of HIPAA to Health Information Exchanges (HIEs) and Electronic Health Records (EHRs) *(by Rob Wilson)*

40

HIEs and EHRs

Approaching HIEs under HIPAA

- First step is to classify the players
  - Participants (data providers and recipients)
  - The exchange itself
  - Vendors and consultants
  - Others (e.g., funding sources)

41

HIEs and EHRs

Approaching HIEs under HIPAA

Participants that are covered entities must apply existing HIPAA **privacy** requirements (as applicable) to activities relating to the exchange

- Uses and disclosures
- Minimum necessary
- Business associates
- Notice of Privacy Practices
- Treatment, payment, and healthcare operations
- Organizational & Admin Reqs/Arrangements
- Authorization
- Consent
- Opt-out
- Other permitted uses and disclosures
- Patients rights
- Mitigation

42

"TPO" (without patient authorization)

- **Covered Entity (and its business associates) may:**
  - Use or disclose protected health information (PHI) for the CE's *own* TPO
- **CE (and its BAs) may disclose PHI:**
  - For treatment activities of a health care provider
  - To another CE for payment activities *of the receiving entity*
  - Regarding a common patient to another CE for *certain* healthcare operations *of the receiving entity*
  - To other CEs participating in a mutual OHCA for health care operations of the OHCA

43

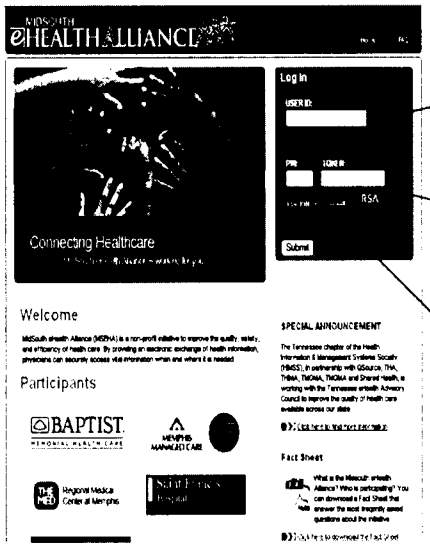
Approaching HIEs under HIPAA

Participants that are covered entities must apply existing HIPAA **security** requirements (as applicable) to activities relating to the exchange, i.e., physical, administrative, and technical safeguards

• Security Mgmt Process	• BA Ks & Arrangements	• Integrity
• Assigned Security Responsibility	• Facility Access Controls	• Person or Entity Authentication
• Info Access Mgmt	• Workstation Use	• Transmission Security
• Awareness & Training	• Workstation Security	• Requirements for Group Health Plans
• Incident Procedures	• Device and Media Controls	• Policies and Procedures
• Contingency Plan	• Access Control	• Documentation
• Evaluation	• Audit Controls	

44

Web Browser Log In



- •User ID: unique eHealth ID (not single sign-on)
- •Token: secure authentication device with changing numerical pin
- •Pin: user creates a unique 4-digit pin number

45

HIEs and EHRs

Approaching HIEs under HIPAA

Is the exchange an entity, or just a set of agreements among participants and vendors?

- If not entity, identify who is doing what at entity level(s). For example, an entity may be a covered entity providing data, but also acting as a BA. Outside vendors may be providing services as BAs.
- If entity, a covered entity, business associate, or both?
- Covered entity?
  - Provider (engaged in transactions), health plan, Medicare Rx drug sponsor?
  - **Health care clearinghouse?**

46

HIEs and EHRs

HIEs as CEs

Health care clearinghouse means a public or private entity, including a billing service, repricing company, **community health management information system or community health information system**, and "value-added" networks and switches, that does either of the following functions:

(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

45 CFR §160.103 (emphasis added)

47

HIEs and EHRs

Approaching HIEs under HIPAA

- **If exchange is a covered entity:**
  - Apply HIPAA concepts/requirements
    - Ignoring inapplicable ones (e.g., for treatment providers and health plans)
    - Still must still consider whether acting as a business associate (and attendant obligations)

48

HIEs and EHRs

Approaching HIEs under HIPAA

Whether exchange is a covered entity or not, is it a business associate?

Generally, "business associates" include:

- Contractors, and
- Other non-employees . . .

Who, on behalf of the Covered Entity, perform or assist with a function or activity involving access to protected health information possessed by the CE

(Decision Tree resource is attached to outline)

49

HIEs and EHRs

Approaching HIEs under HIPAA

If HIE is BA:

- BA Agreement
- Identify functions and activities which BA can perform as if it were the covered entity itself
  - Revisit "treatment, payment, and healthcare operations" permitted uses and disclosures that do not require patient authorization

50

"TPO" (45 CFR § 164.506(c))

- **Covered Entity (and its business associates) may:**
  - Use or disclose protected health information (PHI) for the CE's *own* TPO
- **CE (and its BAs) may disclose PHI:**
  - For treatment activities of a health care provider
  - To another CE for payment activities *of the receiving entity*
  - Regarding a common patient to another CE for *certain* healthcare operations *of the receiving entity*
  - **To other CEs participating in a mutual OHCA for health care operations of the OHCA**

51

HIEs and EHRs

Approaching HIEs under HIPAA

If HIE is BA:

- BA Agreement
- Identify functions and activities which BA can perform as if it were the CE itself
- Consider effect of minimum necessary standard (HHS FAQ # 252 says required in BAAs even though not expressly provided under Standards)
- Identify functions and activities BA can perform for its proper management and administrative purposes
- If problem area, consider HHS FAQ #256 guidance possibly permitting BA uses necessary "in order to provide its service"
- Determine whether HIE will perform aggregation services for multiple covered entities (see definitions for tie to health care operations purposes); especially if no OHCA

52

HIEs and EHRs

Approaching HIEs under HIPAA

Notes re: purposes of uses and disclosures:

- If HIE-related disclosures are for treatment only (or certain TPO activities), no patient authorization is technically required (under HIPAA). Remember to review minimum necessary standard if for payment or operations purposes.
- If disclosure is for research, public health reporting, etc., the applicable elements of HIPAA apply to each access/disclosure.
- If disclosure is for multiple purposes, each purpose must be addressed separately.

53

HIEs and EHRs

Approaching EHRs under HIPAA

- Classify the players:
  - Covered entity is typically user and third party vendors act as business associates
- Uses and disclosures by business associates should be reviewed same as above for exchanges
  - If gray area (e.g., whether covered function or whether info is sufficiently de-identified), covered entities are the ones on the hook and should have final say

54

Case Law Updates
and
Prospects for Amendments
(Research by Phyllis Granade and Nestor Rivera – see outline)

55

Questions?

Phyllis F. Granade
Carlton Fields, P.A.
One Atlantic Center
1201 W. Peachtree St. NW, Ste. 3000
Atlanta, GA 30309
(404) 815-2701 direct
pgranade@carltonfields.com

Robert Q. Wilson
The Bogatin Law Firm, PLC
1661 International Place Drive, Suite 300
Memphis, Tennessee 38120
(901) 767-1234
rwilson@bogatin.com

56