IMPACT OF HITECH ON PHYSICIAN PRACTICES

1

Presenters

EpsteinBeckerGreen
1227 25th Street, NW
Suite 700
Washington, DC 20037
Phone: 202-861-1823
gbreen@ebglaw.com

George B. Breen
Member of the Firm

George B. Breen is a Shareholder of Epstein Becker & Green, P.C. and a member of its Health Care and Life Sciences and Litigation practices. He is co-chair of the firm's Litigation and Government Investigations practice group. Mr. Breen represents clients in connection with matters brought by the U.S. Department of Justice, the Department of Health and Human Services' Office of the Inspector General, State Attorneys General and other state and federal agencies. He also counsels clients on, and litigates, privacy, security and data breach matters.

Mr. Breen speaks and writes frequently about issues related to privacy, security and health care litigation. He is Peer Review Rated "AV" by the Martindale-Hubbell Law Directory and was named an "Outstanding Healthcare Litigator" by *Nightingale's Healthcare News* in its January 2010 Special Report.

2

St. Luke's Health System
190 E Bannock Street
Boise, ID 83702
208-381-5039
doeringh@slhs.org

Herman Doering HIPAA SME
Information System Security Officer

- In February, 2009, joined St. Luke's Health System.
- Member of the Idaho Health Data Exchange Privacy and Security subcommittee of the Board.
- Previously served as Sr. Consultant and HIPAA Subject Matter Expert (SME) with BEST Consulting; Venturi Technology Partners; and COMSYS from 1999 - 2009.
- Provided consulting on Transactions and Code Sets, the Privacy Rule and the Security Rule.

3

St. Luke's Health System
190 E Bannock Street
Boise, ID 83702
208-493-0383
teicheid@slhs.org

Danna Teicheira, CHC, CCEP
System Privacy Officer

- Joined St. Luke's Health System January 2010.
- Member of the Idaho Health Data Exchange Privacy and Security subcommittee of the Board.
- Acting Compliance Officer and Compliance Specialist for Southcentral Foundation, Anchorage, AK
- Manager for Compliance Education and Audit and IDX Functionality Trainer for Tulane Faculty Group Practice, New Orleans, LA

4

Purpose of Presentation

- Provide an update on the HITECH ACT (Part of ARRA)
  - Legal Perspective on the Impact of HITECH
  - Security Officer Perspective on the Impact of HITECH
  - Privacy Officer Perspective on the Impact of HITECH

5

FORMAT

- The legal/regulatory climate
  - Breach Notification
  - Other provisions of HITECH
- Security Issues and Opportunities
  - Challenges
  - New technology
  - Managing Risk
- Privacy Considerations
  - Ensuring compliance
  - Access and disclosure
  - Case Studies – Interactive Session

6

- HIPAA (Health Insurance Portability and Accountability law, codified in the Code of Federal Regulations. The HIPAA regulations are commonly known as:

The **HITECH Act** (Part of ARRA the American Recovery and Reinvestment Act of 2009) expands HIPAA.

7

- The Privacy Rule sets the standards that should be followed to become HIPAA-compliant, but it is the HITECH Act that provides further details regarding HIPAA compliance, emphasizes accountability, and sets penalties for those involved in sharing or accessing PHI.

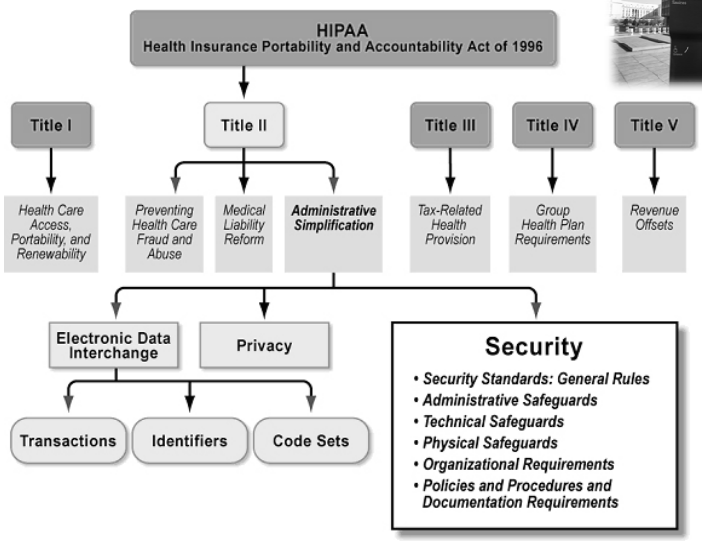
8

- ARRA HITECH Act is concerned with defining the requirements for being compatible with the security and privacy regulations of the Privacy Rule.
- HITECH also facilitates the expansion of HIPAA Act EMR standards that aid in electronic exchange of health information on a national basis to make medical care more organized and transparent.

Source: HIPAA HITECH Act Summary http://whatishipaa.org/hitech-act.php Accessed 9-3-10

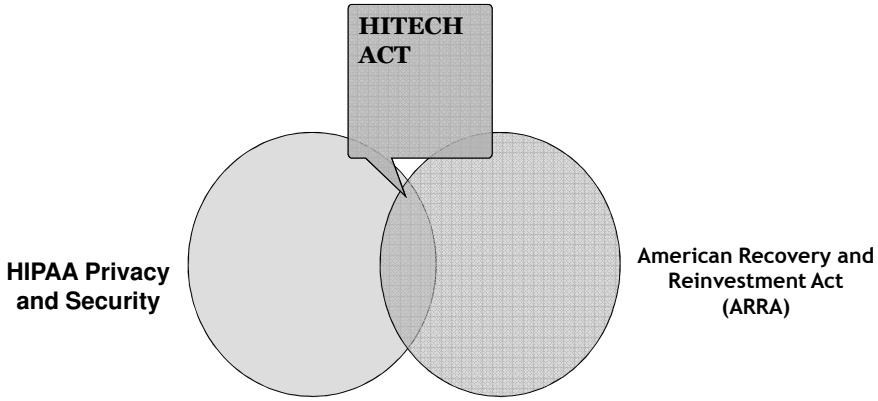
9

HIPAA



10

Sorting it Out: HIPAA; ARRA; HITECH



Unrelated security issues: FTC "Red Flag" Rules around "creditors" having identity theft programs. ARRA incentives for meaningful use or rules for certifying EHRs not subject of this presentation.

11

Four Drivers of Increased Risk

- Direct application of HIPAA's Title II Security rule to Business Associates (BA's)**
- New Breach Notification Requirements under ARRA* (HITECH Act)*
  - Distinct from the Act's attempt to encourage adoption of Electronic Health Records ("EHR"s) by incentive payments for "meaningful use"
- New State Enforcement Authority Under HIPAA and Trend of State Legislated Private Rights of Action
- Government Audits

*Health Information Technology for Economic and Clinical Health (HITECH) Act, as part of the stimulus package (a.k.a. American Recovery and Reinvestment Act (ARRA) of 2009).

** A business associate is a third party that acts on behalf of a covered entity by performing a function or activity that HIPAA's Administrative Simplification rules regulate or that provides certain services (e.g., legal or consulting services) that involve the use or disclosure of individually identifiable health information otherwise known as protected health information ("PHI").

12

Other HITECH Impacts

- Extension of Key Security Provisions to Business Associates
  - Direct exposure to HIPAA civil and criminal penalties
- Penalties increased and "willful neglect" standard now included
- HHS Secretary, based on recommendations from the GAO Comptroller, required to develop mechanism whereby harmed individuals may obtain a percentage of the penalties by February 17, 2012

13

Other HITECH Impacts

- Restrictions on certain disclosures require changes to policies, training and forms:
  - Accounting of certain PHI disclosures
  - Sale of health information
  - Access to information in electronic format
  - Fund-raising opt-out requirement
  - New restrictions on marketing

14

Background on Breach Reporting

- **On August 24, 2009, HHS published regulations** clarifying the breach reporting obligations and providing guidance on the meaning of "secured" and "unsecured" PHI (the "Breach Notification Rules").
- The Secretary delayed enforcement of these regulations in order to give Covered Entities and Business Associates a reasonable amount of time to come into compliance with the breach reporting obligations.
- Enforcement date for ***breach reporting:*** February 22, 2010.

15

Breach

- In the event of a "breach" of "unsecured" PHI, a Covered Entity must notify each individual whose unsecured PHI has been, or is reasonably believed to have been, breached.
- "Breach" is "the acquisition, access, use, or disclosure" of PHI in a manner that violates the Privacy Rule or Security Rule and which "compromises the security or privacy of the [PHI]."
- "Unsecured" PHI is PHI that is "not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary."

16

Reporting Standard

- Statute: "unauthorized acquisition, use or disclosure…which compromises the security, privacy or integrity (of PHI)"
  - Exceptions where inadvertent disclosure to or by workforce, BA or organized health care arrangement participant.
- Regulation: does the breach compromise the security or privacy of the PHI and "pose a significant risk of financial, reputational, or other harm to the individual"

17

Risk of Harm Standard

- The risk of harm standard requires that a Covered Entity undertake some form of risk assessment in the event of a breach, and based upon the assessment, determine in good faith whether it is necessary to notify the individual of the breach.
- The preamble to the Breach Notification Rules specifically references a 2007 OMB Memorandum (M-07-16) "for examples of the types of factors that may need to be taken into account in determining whether an impermissible use or disclosure presents a significant risk of harm to the individual."

18

Risk of Harm Analysis

- The 2007 OMB Memorandum includes the following factors:

1) Nature of the Data Elements Breached.

2) Likelihood the Information is Accessible and Usable.

3) Likelihood the Breach May Lead to Harm.

4) Ability of the Entity to Mitigate the Risk of Harm.

19

Notice Requirements

- Notice must be made to the affected individuals "without unreasonable delay and in no case later than 60 calendar days after discovery of a breach."
- A breach is considered to be "discovered" by the entity as of the first day on which the breach is known to the entity, or should have been known to the entity if it had exercised reasonable due diligence.

20

Notice Requirements

- The notice must:
  - Be in writing, except under circumstances where the Covered Entity does not have the correct contact information for the affected individual, or if there is particular urgency to the notification.

21

Notice Requirements

- The notice must include the following 5 elements:
  1. A brief description of what occurred with respect to the breach, including, to the extent known, the date of the breach and the date on which the breach was discovered;
  2. A description of the types of unsecured PHI that were disclosed during the breach;
  3. A description of the steps the affected individuals should take in order to protect themselves from potential harm caused by the breach;
  4. A description of what the Covered Entity is doing to investigate and mitigate the breach and to prevent future breaches; and
  5. Instructions for the individual to contact the Covered Entity.

22

Notice Requirements

- If the breach of unsecured PHI involves more than 500 residents of a state, the Covered Entity must notify media outlets within that state.
- The Covered Entity must also notify the Secretary of any breach involving 500 or more people.
  - Notification through the media and to the Secretary must be made within 60 days of the discovery of the breach.

23

Notice Requirements

- If the breach involves fewer than 500 individuals, the Covered Entity shall create a log documenting the breach.
  - The Covered Entity shall provide a copy of the log of all breaches to the Secretary within 60 days after the end of each calendar year.
- If the breach occurs at or through a Business Associate, the Business Associate must notify the Covered Entity of the breach *within* 60 days of discovering the breach so that the Covered Entity is able to comply with its breach reporting obligations.

24

Civil Penalties: A Tiered Approach

Level of Intent	Penalty per violation	Maximum Yearly Penalty
Without Knowledge	$100 - $50,000	$1,500,000
Based on reasonable cause	$1,000 - $50,000	$1,500,000
Willful neglect	$10,000 - $50,000	$1,500,000
Willful neglect, not corrected	$50,000	$1,500,000

25

Civil Penalties

- In other words—
  - Penalties for a violation of the Privacy and Security Rule would range from $100 to $50,000 per violation and a per calendar year limit of $1.5 million for each violation of an identical provision of the Privacy or Security Rule.

26

Criminal Penalties (SSA 1177)

Sec. 1177. [42 U.S.C. 1320d-6]

(a) **Offense.— A** person who knowingly and in violation of this part—

(1) uses or causes to be used a unique health identifier;

(2) obtains individually identifiable health information relating to an individual; or

(3) discloses individually identifiable health information to another person, shall be punished as provided in subsection (b).

(b) **Penalties.—** A person described in subsection (a) shall—

(l) be fined not more than **$50,000,** imprisoned not more than **1 year,** or both;

(2) if the offense is committed under false pretenses, be fined not more than **$100,000,** imprisoned not more than 5 **years,** or both; and

(3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, -personal gain, or malicious harm, be fined not more than **$250,000,** imprisoned not more than **10 years,** or both

27

Business Associates

- Business Associates must comply with extensive HIPAA security rule requirements
  - Security officer
  - Security risk assessments
  - Written Business Associate Agreements
  - Written policies
  - Training of workforce members
  - Report security breaches
- Business Associates are subject to the same penalties for non-compliance

28

Business Associate Obligation for Breach Notice

- Must report to Covered Entity without unreasonable delay and no later than 60 days after discovery
- Covered Entity has obligation to report to individuals, Medicaid, HHS

29

BA Agreements – Selected Issues

Issues Include:

- Timing of reporting
- What to report: "can BA make determination of no reasonable likelihood of information being retained?" What if BA disagrees with CE's conclusion?
- Overlap with "incident" reporting?
- For self-funded CEs, who reports?
- CEs seek indemnification (what damages?)
- BAs seek limitation on damages
- Information to be provided in report
- New attention to audits (routine or incident driven

30

BA Agreements – Selected Issues

- Information to be provided in report
- New attention to audits (routine or incident driven
- Must be updated in light of HITECH Act changes
- Be careful regarding indemnity & insurance provisions
- Re-evaluate who your business associates are and get updated agreements in place

31

Pre-HITECH Enforcement: HHS Enforcement

- **Privacy and Security Rules are enforced by HHS' Office for Civil Rights (OCR) and CMS**
  - OCR and CMS had reportedly resolved over 6,700 Privacy and Security Rule cases by requiring the entities to make systematic changes to their health information privacy and security practices, without monetary penalties before the first Resolution Agreement was announced.

32

Pre-HITECH Enforcement

- **HHS and Providence Health & Services Reach Resolution Agreement including Corrective Action Plan to Protect Health Information- July 2008**
  - First time HHS required a monetary payment and a Resolution Agreement.
  - Enforcement stems from repeated incidents at Providence facilities where unencrypted backup tapes, optical disk, and laptops, all containing health information, were removed from the premises and left unattended.

33

Pre-HITECH Enforcement

- Under the Resolution Agreement, Providence agreed to pay $100,000 and implement a Corrective Action Plan.
- **CMS Spokeswoman**: "This resolution confirms that effective compliance means more than just having written policies and procedures. To protect the privacy of patient information, covered entities need to continuously monitor the details of their execution, and ensure that these efforts include effective privacy and security staffing, employee training and physical and technical features."

34

Pre-HITECH Enforcement

- **Providence Health & Services Resolution Agreement:**
  - Three year term.
  - Preserves HHS' right to seek Civil Monetary Penalties.
  - Tolling of the Statute of Limitations.
  - Corrective Action Plan Requires:
    - HHS approval of policies and procedures;
    - Annual policy review;
    - Evidence of policies and procedures distribution;
    - Training of workforce; and
    - Annual Reports to HHS.

35

Pre-HITECH Enforcement

- **January 16, 2009, CVS accepted $2,250,000 penalty and Corrective Action Plan (CAP) to settle complaint stemming from its practice of disposing of old prescriptions and prescription bottles.**
- **The CAP requires**:
  - Revising and distributing policies and procedures regarding disposal of protected health information; extensive minimum content prescribed; must be approved by HHS;
  - Sanctioning workers that do not follow the policies and procedures;
  - Training workforce members on these new requirements;
  - Conducting internal monitoring;

36

Pre-HITECH Enforcement

The CAP Also Requires:

- Engaging a qualified, independent third-party "Assessor" to conduct assessments of CVS' compliance with the requirements of the CAP and render reports to HHS;
- Implementation Report and Annual Reports including attestations;
- New internal reporting procedures requiring workers to report all violations of these new privacy policies and procedures;
- Three year term;
- Breach provisions: Breach of CAP is breach of Resolution Agreement; ongoing obligation to cure; potential imposition of Civil Monetary Penalties; Tolling of Statute of Limitations.

37

Current Enforcement Efforts: Rite-Aid Pharmacy

- July 27, 2010, Rite-Aid agreed to pay $1,000,000 to HHS and enter into a Corrective Action Plan (CAP) to settle a complaint stemming from its practice of disposing of prescriptions and labeled pill bottles.
- In a coordinated action, Rite Aid also signed a consent order with the Federal Trade Commission (FTC) to settle potential violations of the FTC Act

38

Current Enforcement Efforts: Rite-Aid Pharmacy

- The CAP requires:
  - Revising and distributing its policies and procedures regarding disposal of protected health information and sanctioning workers who do not follow them;
  - Training workforce members on these new requirements;
  - Conducting internal monitoring;
  - Engaging a qualified, independent third-party assessor to conduct assessments of Rite-Aid's compliance with the requirements of the CAP and render reports to HHS;
  - Rite Aid has also agreed to external, independent assessments of its pharmacy stores' compliance with the FTC consent order.
- The HHS corrective action plan will be in place for three years; the FTC order will be in place for 20 years.

39

New Enforcement Authority under HITECH – State Attorneys General

- **Under new section to HIPAA - 42 USC 1320d-5(d)):**
  - State Attorneys General can bring civil actions in federal court on behalf of state residents "threatened or adversely affected by" a violation of the HIPAA Privacy or Security Rules.
  - Available remedies and sanctions: injunctive relief; statutory damages of $100 per violation, not to exceed $25,000; and attorneys' fees and costs.
  - State Attorneys General are required to serve prior written notice on the Secretary of HHS, where feasible, in which case HHS can intervene in the action.
  - If HHS brings prior action, it preempts an identical state action to enforce HIPAA.
  - However, State Attorneys General remain able to bring actions under their own state laws that are not in conflict with HIPAA.

40

New Enforcement Authority under HITECH – State Attorneys General

- State Attorneys General are required to serve prior written notice on the Secretary of HHS, where feasible, in which case HHS can intervene in the action.
- If HHS brings prior action, it preempts an identical state action to enforce HIPAA.
- However, State Attorneys General remain able to bring actions under their own state laws that are not in conflict with HIPAA.

41

Post-HITECH: First Reported State Enforcement - *CT v. Health Net*

- **Complaint Allegations:**
  - May 2009 - Health Net learns of lost portable disc drive with financial and PHI information of approx. 446,000 current and former CT enrollees.
  - November 2009 – Health Net notifies CT enrollees.
- **January 2010 - CT AG files suit:**
  - **3 Causes of Action Pled:**
    1. Failure to comply with HIPAA.
    2. Violation of CT Unfair Trade Practices Act.
    3. Civil Penalties for Willful Violation of CT Unfair Trade Practices Act.

42

Post-HITECH: First Reported State Enforcement - *CT v. Health Net*

- **Relief Sought:**
  - Injunctive relief under HIPAA and CT State law; Statutory damages for HIPAA violations, including costs and attorneys fees under HITECH; State CMPs (up to $5,000 per willful violation) and attorneys fees and costs under CT State law.

43

Stipulated Judgment

- Parties agree to entry of Stipulated Judgment on July 7, 2010
  - **Judgment provides for:** Guaranteed Payment of $250,000.00 to the State of Connecticut, with a contingent obligation to pay $500,000.00 if certain events occur
  - Institution of a Corrective Action Plan which requires HealthNet to:
    - encrypt all laptops and desktops
    - train employees on encryption, storage and removable media
    - annual employee training
    - provide 2 years of Identity Theft Protection for affected members at HealthNet's expense
  - If any member experiences identity theft, to provide services to restore the member's identity at no cost to member
- Stipulated Judgment reflects that HealthNet had incurred $7 million in costs in connection with the data breach

44

Implications of State HIPAA Enforcement Authority

- State Attorneys General Have a Track Record of Privacy Enforcement, Including Health-Related Information
- 45 States with Security Breach Notification Laws Covering Personally Identifiable Information (PII) (for a summary of those state laws see **http://law2point0.com/wordpress/2009/09/15/50-state-security-breach-notice-law/**)
- Several of these states now have medical and health-related breach notification statutes (e.g., **AR**, **CA, MO, TN,** & **NH)**

45

Likelihood of State AG Enforcement

- HITECH requires individual and media notification for large breaches - AGs will monitor notices and coordinate action
- If no notification is required under HITECH, state AG's have other ways of learning of breaches:
  - State medical or financial breach notification laws
  - Impacted consumers
  - Employees
  - Investigations/audits (CID authority)
- State consumer protection statutes can up-the-ante
- AG priorities: is entity doing everything feasible to protect residents from a breach (e.g., security policies and practices) and to enable residents to protect themselves in the event of a breach (e.g., notification, mitigation after breach)?

46

Other Enforcers Efforts

- **Kaiser Permanente Northern California - January 2010**
  - Medical records for about 15,500 N. California patients were compromised
  - An external hard drive was stolen from an employee's car
  - Employee was authorized to use medical records data, but should not have used an external drive
  - AG has begun an investigation and will likely fine Kaiser for the breach
  - Potential costs and fines are estimated at around $2 million

47

Other Enforcers Efforts

- **Blue Cross/Blue Shield Tennessee - October 2009**
  - 58 hard drives were stolen from a training facility
  - The hard drives contained audio and video files with identifying information for nearly 1M members
  - The plan is notifying members about the data theft and is offering no-cost credit monitoring to individuals
  - The plan has hired 700+ contractors and employees to help determine what data was contained on the hard drives
  - Costs already more than $7M, and the plan will incur more as identity protection services are offered
  - The plan notified AGs in 32 states about the breach

48

Proposed Modifications to HIPAA under the HITECH Act

New regulations proposed by DHHS on 7/8/10. Highlights:

- *Business Associates Have Direct Liability*
  - The standards, requirements, and implementation specifications of some of the HIPAA Rules now directly apply to business associates.
  - Business associates can be held civilly and criminally liable for penalties for violations of those requirements.
- *Subcontractors are Deemed Business Associates*
  - Subcontractors of a covered entity's business associates are also considered business associates to the extent that they require access to PHI.

49

Proposed Modifications to HIPAA under the HITECH Act

- *Existing Business Associate Agreements Must be Updated - New Provisions*
  - Business Associate must report breaches of unsecured PHI to the covered entity
  - Business Associate will be compliant with the applicable provisions of the Security Rule
  - Business Associate will enter into business associate agreements with its subcontractors
- Note: Covered Entity still directly liable for certain violations of HIPAA even if the violation is the fault of the business associate.
- *Additions to Notice of Privacy Practices and Ability to Request Restriction of Use of PHI*
- **Effective Date - January 7, 2011**

50

Are You Ready for an Audit?

- OCR work plan calls for audits
- Notice of breach will trigger audit
- Customers may negotiate for audit right in BA agreement or require them before contracting
- Who will be interviewed?
  - President, CEO, and Directors
  - HIPAA Compliance Officer
  - Lead Systems Manager or Director
  - Systems Security Officer
  - Disaster Recovery Specialist
  - Person in charge of data backup
  - Facility Access Control Coordinator
  - Human Resources Representative
  - Director of Training
  - Incident Response Team Leader

51

Documents Likely to be Requested During an Audit

- Entity-wide security plan
- Most recent risk analysis
- Risk management plan
- Security violation monitoring reports
- Vulnerability scanning plans:
- Results from most recent scan
- Network penetration testing policy and procedure
  - Results from most recent network penetration test
- List of all user accounts with access to systems which store, transmit, or access ePHI (for active and terminated employees)
- Configuration standards to include patch management for systems which store, transmit, or access ePHI
- Organizational chart to include staff members responsible for general HIPAA compliance to include the protection of ePHI

52

Documents Likely to be Requested During an Audit

- Examples of training courses or communications delivered to staff members to ensure awareness and understanding of ePHI policies and procedures
- Policies and procedures governing the use of virus protection software
- Disaster recovery plan
- Data backup procedures
- Analysis of information systems, applications, and data groups according to their criticality and sensitivity
- Inventory of all information systems to include network diagrams listing hardware and software used to store, transmit, or maintain ePHI
- List of all Primary Domain Controllers (PDC) and servers
- Inventory log recording the owner and movement of media and devices that contain ePHI

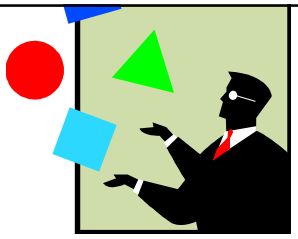
53

Specific Policies and Procedures Requested During a Security Audit*

- HHS Officials policies request includes:
  - Access Control Policy
  - Business Continuity Policy
  - Risk Analysis Policy
  - Compliance Policy
  - Data Transmission Policy
  - Security Incident Tracking Policy
  - Information System Monitoring Policy
  - Physical and Environmental Security Policy
  - Computer Use Policy
  - Wireless Network Security Policy
  - Firewalls, routers and switches
  - Information Systems Management Policy
  - Data Encryption Policy
  - Data Sanitization Policy

* OIG was interested in all these at Piedmont Healthcare

54



Physicians and Security

A Balancing Act:
Physician expectations, technology, and heightened security standards

55

Security is a balancing act

- Physician Practices are challenged to
  - Meet physician/provider expectations regarding new technology, including EMRs, EHRs, specialty-specific software, as well as blackberries and other PDAs
  - Evaluate and make decisions regarding acquisition, installation, and maintenance of new technologies
  - Comply with stricter security regulations in order to protect the organization and the physicians

56

Security is a balancing act

- Information Security Officers are tasked with assuring compliance with many laws and regulations and that the selected information technologies also comply.

  There are several challenges here:
  1) Understanding that Information Security Officers must be involved in the decision-making
  2) The problems with "after the fact" requests for evaluations
  3) Protecting the flow of Protected Health Information internally and externally

57

58

10 Security Concepts

1. **Information Access**
   - Access only the minimum amount needed
   - Don't access information on patients who are not under your care
   - Inappropriate access can subject you to disciplinary action on up to dismissal
2. **Incident Reporting**
   - Need to be able to identify and report incidents promptly
   - Types of incidents include loss of data, alteration, hacking, wrong disposal of computer equipment

10 Security Concepts, cont.

3. **Physical & Workstation Security**
   - Ensure visitors are identified and not allowed in restricted areas, no locked doors left open, report suspicious activity, keep PHI documents secured and out public sight
   - Turn PC screens away from public areas or where can easily be seen; put PHI documents face down when not in use or faced against the wall in chart holders; archive patient information in locked cabinets; use screensavers, auto timeouts, privacy screens; beware of the internet, only visit business related sites
   - Know what to do during System downtimes

59

10 Security Concepts, cont.

4. **Password Management**
   - Protect them, your logon ID/Password combination is your signature, choose a strong password, regularly expire them. Never use vendor default passwords.
5. **Email Security**
   - Internal vs. external security and encryption, using correct addresses, who should get them, copying and forwarding, unknown parties

60

10 Security Concepts, cont.

6. **Fax Security**
   - Recipients Fax number, follow-up, cover sheets, pickup times, unclaimed
7. **Document Retention and Destruction**
   - Keep only as long as needed, handling PHI documents, plastic media, magnetic media
8. **Offsite/Telecommuting**
   - Protect portable devices, transporting, encryption, storage, information

61

10 Security Concepts, cont.

9. **Confidentiality Agreements**
   - Sign at hire and then annually
10. **Security Policies**
   - Must have the HIPAA required policies and procedures written, available, and training provided to all workforce members including sanctions for violations

62

Business Associate Risk

- A November 2009 HIMSS Analytics report* found that Business Associates were generally not prepared to meet the new data breach HITECH obligations.
  - How many BA's do you have?
  - What actions would you take if they breached your data?

❖ 2009 HIMSS Analytics Report: Evaluating HITECH's Impact of Health care Privacy and Security sponsored by ID Experts, page 4

63

Data Loss Prevention (DLP)

- This tool can be set to monitor, encrypt, quarantine or block ePHI data and even halt a potential breach as it is taking place
- It does this through real-time flags and notifications that can be sent to the person involved and notifies the Information Security Officer
- Physician practices can now get this technology as well as hospitals

64

Auditing and monitoring

- Auditing and monitoring continue to be important tools in relation to meeting HITECH and HIPAA requirements
- Remember, auditing and monitoring is one of the seven (7) elements of a Compliance Plan (both OIG and Federal Sentencing Guidelines (FSG) – link to proposed FSG amendments
  - http://www.ussc.gov/2010guid/20100503_Reader_Friendly_Proposed_Amendments.pdf -- look on page 33 (effective 11/01/10)

65

Threats to Security

- The just released 2010 Verizon/US Secret Service Data Breach Investigations Report identifies the growing threats to information security
- Findings worldwide include: 70% of the data stolen resulted from external criminal organization agents, and 48% was caused by insiders
- How breaches occurred breaks down as follows: 48% due to privilege misuse, 40% from hacking, 38% from malware
- 98% of all data breached came from servers, 85% of attacks were not considered highly difficult, 61% were discovered by a third party
- Where should security efforts be focused? Eliminate unnecessary data; keep tabs on what's left; Ensure essential controls are met, test and review web applications, audit user accounts and monitor privileged activity

66

Threats to Security

- Health Net just recently settled the first lawsuit filed under the HITECH Act for the loss of a hard drive holding 500,000 enrollee records and paying $250,000, agreeing to a CAP, and to another $500,000 fine if the drive is accessed and personal information is used illegally
- The Russians have come out with new software to virtually hack any system starting at $50. You can buy it on the Internet
- Specifics for physicians to consider–
  - The need for "instant access" must be balanced with security
  - Reluctance to use more complex passwords
  - Lack of knowledge regarding security policies

67

With HITECH funding comes Whistleblower protections

- The ARRA whistleblower protections are very broad in scope. The protections apply to employees of non-federal employers receiving funds under ARRA. Not unlike many whistleblower statutes, ARRA's provisions prohibit covered employers from discharging, demoting, or discriminating against, an employee who engages in certain protected conduct. The scope of the protected conduct, however, is quite broad. Protected conduct includes disclosing:
  - gross mismanagement of an agency contract or grant relating to covered funds;
  - a gross waste of covered funds;
  - a substantial and specific danger to public health or safety related to the implementation or use of
  - covered funds;
  - an abuse of authority related to the implementation or use of covered funds; or
  - a violation of law, rule, or regulation related to an agency contract (including the competition for or
  - negotiation of a contract) or grant, awarded or issued relating to covered funds.
  - Source: **HITECH Act Fund Recipients at Risk for Whistleblower Claims *Employment Law Alert* Bass Berry Sims PLC (March 29, 2010)** Retrieved from: http://www.bassberry.com/files/Publication/a91645dd-0b30-48a0-a067-01bd97baa8c4/Presentation/PublicationAttachment/4bbec985-28d7-416d-93aa-0606ba90c15d/EmploymentLawAlert29032010.pdf (9/24/10)

68

PRIVACY CONSIDERATIONS

The Human Element

69

Discussion Points

- Elements of Privacy and Security Plan
- Policies and Procedures
- Training
- Investigation/Corrective Action
- Sources – Get Connected, Stay Current

70

What happened here?

- A physician is rounding and notices that a neighbor has been admitted to the floor.
  - The physician accesses the neighbor's record and finds that the neighbor is critically ill.
  - The physician shares information regarding the neighbor's condition with a mutual friends for a good reason: the physician wants the mutual friend to have the opportunity to visit and possible "say goodbye."
  - The hospitalized neighbor receives a visit from the concerned friend.
  - The physician is contacted by the Privacy Officer regarding an alleged access and disclosure of Protect Health Information.

71

What happened here?

- A private practice failed to honor an individual's request for a complete copy of her minor son's medical record. …the private practice had relied on state regulations that permit a covered entity to provide a summary of the record.
- OCR's Response: OCR provided technical assistance to the covered entity, explaining that the Privacy Rule permits a covered entity to provide a summary of patient records rather than the full record only if the requesting individual agrees in advance to such a summary or explanation. Among other corrective actions to resolve the specific issues in the case, OCR required the covered entity to revise its policy. In addition, the covered entity forwarded the complainant a complete copy of the medical record.
- Source: OCR Home > Health Information Privacy > Enforcement Activities & Results > Case Examples & Resolution Agreements, Retrieved from:
- http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/allcases.html#case7 (9/23/10)

72

Privacy/Security Plan Basics

- Policies and Procedures
- Training (ongoing)
- Accountability (job descriptions stating compliance is expected)
- Security communications to Staff
- Auditing and Monitoring
- Responding to detected issues
- Pro-actively assessing risk areas
- Corrective Action

Buy-in and Support of Senior Leadership is vital to the success of a Privacy and Security Program.

73

Regulations call for designating a Privacy Officer and a Security Officer

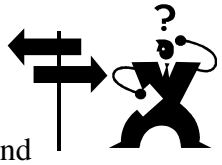
45 CFR § 164.530 Administrative requirements.

- (a)(1) *Standard: Personnel designations.*
- (i) A covered entity must designate a privacy official…. who is **responsible for the development and implementation of the policies and procedures** of the entity.

- **45 CFR § 164.308 Administrative safeguards.**
  - (a) (2) *Standard: Assigned security responsibility.* Identify the security official who is responsible for the **development and implementation of the policies and procedures (emphasis added)** required by this subpart for the entity.

74

Policies and Procedures



- Does your office/organization have Privacy and Security policies?
- Do you know which Privacy and Security policies apply to you?
- Have you received training regarding applicable policies and procedures?
- Do you know where to locate/find policies and procedures?
- Are the policies current?

75

What do policies and procedures do?

- Provide guidance to ensure compliance
- Set expectations and assign accountability
- Provide protection for both the individual and the organization

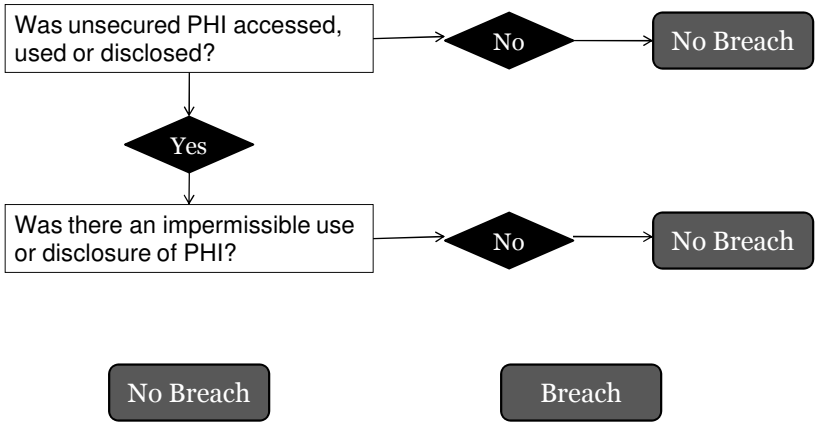
76

Breach Policy

- Do you have one?
- Is it specific as to the steps to take regarding
  - Determining if a breach occurred?
  - Notifying affected Individuals?
  - Handling breaches of more than 500 individuals
- General policies that state something like "in the event of a breach all steps will be taken in accordance with applicable law" may leave you scrambling.

77

Decision Trees are useful (truncated version)



78

The LIST no one wants to be on

79

Source: retrieved from: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html

80

Access, Use, Disclosure

81

Definitions

- ***Disclosure*** means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information. (**external**) 45 CFR **§ 160.103 Definitions.**
.
- ***Use*** means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information. (internal) 45 CFR **§ 160.103 Definitions.**
- **Minimum Necessary**: When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. **§ 164.502 Uses and disclosures of protected health information: general rules.**

82

Office of Civil Rights FAQ

Won't the HIPAA Privacy Rule's minimum necessary restrictions impede the delivery of quality health care by preventing or hindering necessary exchanges of patient medical information among health care providers involved in treatment?
Answer:
No. Disclosures for treatment purposes (including requests for disclosures) between health care providers are explicitly exempted from the minimum necessary requirements. [emphasis added]

Uses of protected health information for treatment are not exempt from the minimum necessary standard [emphasis added].

Source: HHS.Gov Health Information Privacy, Frequently Asked Questions: Retrieved from: http://www.hhs.gov/ocr/privacy/hipaa/faq/minimum_necessary/208.html (9/23/10)

83

Treatment – Know the Definition & Scope

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

84

Distinguishing between Consent and Authorization to disclose Protected Health Information

- **Consent to disclose** is verbal; and not ongoing. The disclosures are in the best interests of the patient (professional judgment).
- **Authorization** is written and can allow broader and ongoing disclosures; HIPAA requires a valid authorization form for disclosures of PHI that fall outside the circumstances involves limited disclosures to individuals involved in the patient's care
- Note: Some disclosures are mandated by State Law and HIPAA permits the disclosure without consent but requires the disclosure be logged.

85

Training and Investigations

86

All reports of Privacy or Security incidents should be investigated and tracked

- The scope of the investigation will be determined by the nature of the allegation/report, the facts provided, and any supplemental evidence (electronic records reports, eyewitnesses, etc).
  - All breaches are HIPAA violations; however, under the current breach regulations, not all HIPAA violations are breaches. That may change if the "harm" test is removed from the breach analysis
- Incidents should be tracked and information reported to senior management/boards/CEO as appropriate for the organization.

87

Encouraging Reporting

- Reporting responsibilities should be clearly stated in a policy
  - Create an environment where the focus of reporting is protecting patients
  - Provide training to staff; they can't comply with law unless they know the behaviors expected
  - Implement consistent corrective action standards

88

SNOOPING: A Growing Concern

- A physician and two healthcare workers pleaded guilty to misdemeanor violations of the health information privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA) based on their accessing a patient's records without any legitimate purpose
  - Physician was sentenced to one year of probation, a $5,000 fine to be paid in 60 days, and 50 hours of community service educating professionals on HIPAA. The other health care workers also received probation and fines.
    - **Source: A Physician and Two Former Hospital Employees Sentenced for HIPAA Violations. *Compliance Home.* Retrieved from: http://www.compliancehome.com/news/HIPAA/16505.html (9/24/10)**
- A former UCLA School of Medicine researcher was sentenced to four months in federal prison for illegally snooping into the confidential private records of celebrities, high-profile patients and co-workers.
  - **Source: UCLA Researcher Gets Jail for Snooping into Celebrity Medical Records. (April 27, 2010) KTLA.com retrieved from: ttp://www.ktla.com/news/landing/ktla-ucla-medical-records,0,5682431.story (9/24/10)**

89

Training: Critical to A Successful Privacy and Security Program

- "As the healthcare industry continues to digest profound HITECH changes to HIPAA Privacy and Security rules, two observations already are apparent and indisputable for covered entities and their business associates. First, time and resources spent on a workforce that is well-trained on the Privacy and Security rules will be an investment of exponential value. Second, enforcement of those same rules will make negligent and uncorrected errors very costly. A well-trained workforce makes fewer mistakes, and identifies and fixes those that it makes. A workforce that violates the rules because it does not know them or does not care to know them makes an inviting target for HITECH's new enforcement initiatives. **The lesson seems clear: train on HITECH and re-train on existing HIPAA rules–or pay some new and onerous penalties for workforce mistakes. (emphasis added)"**
- **Source: HITECH and HIPAA Training: Time to Double Down. HIPAA.com retrieved from: http://www.hipaa.com/2009/11/hitech-and-hipaa-training-time-to-double-down/ (9/24/10)**

90

GET CONNECTED

Stay Current
Stay Compliant

91

Join a Listserv

- Health Information Privacy/ Sign Up for the OCR Privacy & Security Listserv http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/listserv.html
- There are many online resources for HIPAA and HITECH. Professional Organizations (HCCA, SCCE, AHIMA)

92

Go to the Source: HHS Resources

- Health Information Privacy main page: http://www.hhs.gov/ocr/privacy/index.html
- Health Information Privacy FAQs: http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html
- Understanding Health Information Privacy: http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html
- Health Information Privacy/For Covered Entities: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html
- Summary of the HIPAA Privacy Rule: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

93

Go to the Source: HHS Resources

- Summary of the HIPAA Security Rule: http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html
- Health Information Privacy/HIPAA Enforcement: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html
- Breach Notification Final Rule Update http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/finalruleupdate.html
- For Covered Entities http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html

94

Case Studies – Interactive Session

95

Scenario 1: Using electronic health record (EHR) access privileges

- **Situation**: Carol is a RN in a physician's office. The physicians admit patients to a local hospital and Carol has been granted access to its EHR system. Her mother was admitted to this hospital, but is not a patient of the physicians she works for. Carol decides to use her access right to view her own mother's electronic medical records. Is this OK?
- **Response**: No. By accessing this information, Carol will violate the federal HIPAA regulations and her mother's privacy. Carol does not need this information to do her job and would be accessing the information for personal reasons. Such actions may result in disciplinary action as well as termination of Carol's EHR access privileges by the local hospital.

96

Scenario: Request for A Record

- **Situation**: A mental health patient requests a copy of her records. The patient signed a valid authorization, but is denied access to her records. Can the patient be denied access to her records?
- **Response**: Yes and No. HIPAA allows denial of access to records if a provider determines that release of the information would cause substantial harm to the patient or others. The patient (or personal representative) must be informed of the denial and offered the right to appeal. In this particular instance, the patient was not given a notice of the denial and the right to appeal. This was investigated by OCR and OCR determined that the patient was not offered the opportunity to have the denial reviewed.

97

Scenario: Logons

- **Situation**: Kim is an employee of a vendor that provides services to a local hospital. She comes to the hospital accompanied by Jeff. Jeff's access privileges have not yet been activated. Jeff asks Kim if it would be alright for him to temporarily use her Logon until he gets his in a few hours. He reminds her they both have the same deadline to accomplish for the CEO of the hospital by noon. Is this OK under the circumstances?
- **Response**: No. Sharing unique ID's and passwords is a violation of the local hospital's policy and may result in termination of Kim's access privileges at the hospital. Jeff must wait until the hospital completes his access request and he has signed a Confidentiality and Network Access Agreement.

98

Scenario: Business Associates

- **Situation**: A business associate reports that a disgruntled employee (who was subsequently terminated) hacked its network and posted some patient information on a Facebook page. The business associate reported the incident to the covered entity on May 15, 2010. When asked when the posting was discovered, the business associate stated that it knew in January that the posting was up. The stated reason for delay was that the business associate was working through legal channels to get the situation resolved; hence the delay in reporting. What date is the date that the covered entity will use for "knew or should have known?" Is there a reportable breach?
- **Response**: Date of "knew or should have known" for the covered entity is May 15, 2010. Is it a breach? Unknown. Until the business associate provides what information was on the Facebook page, the covered entity cannot determine if a breach has occurred. This issue also raises questions about the business associate contract and what security measures it has taken.

99

Scenario: Accessing Medical Information

- **Situation**: Dr. Parks is employed by the local hospital. Dr. Parks has been granted access to the hospital's EHR for patient care purposes. The football coach of a large state university was recently admitted to the hospital. The coach is not receiving treatment from Dr. Parks. His only reason for accessing the coach's medical records is curiosity or concern for the coach. Is it permissible for Dr. Parks to use his EHR access to look at the coach's records?
- **Response**: No. Dr. Parks will violate federal HIPAA regulations and the coach's privacy. Dr. Parks is not caring for the coach and would be accessing the information for personal reasons. Such actions may result in federal penalties and fines as well as removal of access privileges and medical staff disciplinary action.

100

Scenario: Disposing of Documents

- **Situation**: Jan works for a collection agency that contracts with a pediatric practice. Jan has been provided access to the pediatric practice's patient accounting system in connection with her job. Jan frequently needs to print documents containing patient information. Jan disposes of these documents in the trash marked for recycling, not the regular trash. Is this permissible?
- **Response**: No. All patient and business confidential information must be disposed of in secure manner, either in a locked bin or receptacle for confidential information. Confidential materials must then be destroyed by cross cut shredding or burning. Jan's actions may result in disciplinary action and/or removal of her access privileges by the pediatric practice and possibly termination of the Business Associate agreement with Jan's employer.

101

Scenario: Fax Goes Astray

- **Situation**: Mike works in patient billing. He is contacted by an insurance company who asks that detailed medical information be provided to support a bill for a service. He gathers the information and manually keys in the fax number; the number is preprogrammed, but Mike doesn't want to scroll through the fax number list to find it. He receive a call a hour later from an individual who states he received a fax on his office fax machine. The information went to a florist's office. What actions should be taken to mitigate a possible breach?
- **Response**: Mike should report the incident immediately. Mike or other staff member should attempt to retrieve the fax or at least verify that the florist's shop has a shredder that will allow for compliant disposal of the information. Review what information was released to see if "harm" may have occurred. A sanctions policy should indicate what, if any, corrective action Mike will receive.

102

QUESTIONS?

George B. Breen
EpsteinBeckerGreen
1227 25th Street, NW
Suite 700
Washington, DC 20037
Phone: 202-861-1823
gbreen@ebglaw.com

Herman Doering
St. Luke's Health System
190 E Bannock Street
Boise, ID 83702
208-381-5039
doeringh@slhs.org

Danna Teichera
St. Luke's Health System
190 E Bannock Street
Boise, ID 83702
208-493-0383
teiched@slhs.org

103

IMPACT OF HITECH ON PHYSICIAN PRACTICES

104