HIPAA 101

Scott A. Weinstein
Partner
sweinstein@mwe.com
(202) 756-8671

March 22, 2019
mwe.com
HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

• The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), Public Law 104-191, included Administrative Simplification provisions that required the U.S. Department of Health and Human Services (“HHS”) to adopt federal privacy protections for individually identifiable health information.

• The Privacy Rule, Security Rule, and Enforcement Rule implement certain of the Administrative Simplification provisions.

• HIPAA is enforced by the Office for Civil Rights (“OCR”) within HHS.
Flow of patient-identified health information

Flow of non-identifiable health information

SOURCE: NATIONAL RESEARCH COUNCIL, COMPUTER SCIENCE AND
TELECOMMUNICATIONS BOARD FOR THE RECORD: PROTECTING
ELECTRONIC HEALTH INFORMATION (WASHINGTON, DC: NATIONAL
ACADEMY PRESS, 1997).
STRUCTURE OF PRESENTATION

• The following three regulations form the structure for today’s presentation:

  – **The Privacy Rule** – establishes patients’ privacy rights and addresses the use and disclosure of protected health information (“PHI”) by covered entities (“CE”s) and business associates (“BA”s).

  – **The Breach Notification Rule** – requires HIPAA CEs and their BAs to provide notification following a breach of unsecured PHI.

  – **The Enforcement Rule** – establishes both civil monetary penalties and federal criminal penalties for the knowing use or disclosure of PHI in violation of HIPAA.

• The presentation will also address a recent Request for Information published by the U.S. Department of Health and Human Services Office for Civil Rights (OCR), which could affect certain provisions of the Privacy Rule.
RECENT HIPAA REQUEST FOR INFORMATION (RFI)

• On December 14, 2018, OCR published an RFI that seeks feedback on whether and how the HIPAA Privacy Rule should be revised

• Primary goal of RFI - to identify whether certain HIPAA provisions unnecessarily “limit or discourage information sharing needed for coordinated care or to facilitate the transformation to value-based health care”

• RFI suggests that OCR is considering the first significant changes to the HIPAA Privacy Rule since January 2013

• Comment period ended on February 12, 2019
PRIVACY RULE: OVERVIEW

• Major Goal:
  – “[A]ssure that an individual’s health information is properly protected while
    allowing the flow of health information needed to provide and promote high
    quality health care and to protect the public’s health and well-being.”

• HIPAA Privacy Rule:
  – Governs what persons are subject to requirements, what type of information
    that is protected, and when protected information may be used or disclosed.
  – Contains rules about patient rights.
  – Contains rules about administrative requirements.
PRIVACY RULE: WHO IS A “COVERED ENTITY”? 

The HIPAA Privacy Rule applies to CEs.

• **Health Plans:** Individual and group health plans that provide or pay the cost of health care.

• **Health Care Providers:** Health care providers, regardless of size, who electronically transmit health information in connection with certain “standard” transactions covered by HIPAA.

• **Health Care Clearinghouses:** Entities that process non-standard information they receive from CEs into a “standard” format (or vice versa).
PRIVACY RULE: WHO ELSE IS COVERED?

• **Organized health care arrangements (“OHCA”):**
  – Multiple CEs holding themselves out to the public as participating in joint arrangements or activities.

• **Business Associates:**
  – An individual or entity that “creates, receives, maintains, or transmits PHI for a function or activity” on behalf of a CE or OHCA, but other than as a part of the workforce of the CE or OHCA.
  – A good example is a billing and collection company that creates, receives, maintains, or transmits PHI on behalf of a CE.
 PRIVACY RULE: WHAT INFORMATION IS PROTECTED?

• The HIPAA Privacy Rule applies to “Protected Health Information”.

• “Protected Health Information” or “PHI” is:
  – “Individually identifiable health information” held or transmitted by a CE or its BA, in any form or media, whether electronic, paper, or oral.

• “Individually Identifiable Health Information” is:
  – Information that relates (1) to individual’s past, present or future physical or mental health condition, (2) to provision of health care to the individual, or (3) to past, present, or future payment for the provision of health care to the individual; and
  – Identifies the individual or could reasonably be used to identify the individual.
PRIVACY RULE: WHAT INFORMATION IS PROTECTED? (CONT.)

• PHI does not include “de-identified” information.

• 2 ways to de-identify information:
  – formal determination by a qualified statistician; or
  – removal of the following 18 specific identifiers:

| (1) Name | (10) Dates (e.g., birth dates) |
| (2) Geographic subdivisions smaller than a state | (11) Fax numbers |
| (3) Telephone numbers | (12) Email addresses |
| (4) Social security numbers | (13) Medical record numbers |
| (5) Health plan beneficiary number | (14) Account numbers |
| (6) Certificate/license numbers | (15) Vehicle identifiers and serial numbers |
| (7) Device identifiers and serial numbers | (16) URLs |
| (8) Internet protocol (IP) addresses | (17) Biometric identifiers |
| (9) Full-face photographs/images | (18) Other unique identifiers |
PRIVACY RULE: GENERAL RULE

• A CE may not use or disclose an individual’s protected health information, except as:
  – (1) otherwise specifically permitted or required by HIPAA; or
  – (2) as authorized by the individual who is the subject of the information.
PRIVACY RULE: REQUIRED DISCLOSURES

• CEs **must** disclose PHI:
  – To individuals (or their personal representatives) in connection with an access or accounting request about the individual’s PHI.
  – To HHS in connection with a compliance investigation, review, or enforcement action.
PRIVACY RULE: PERMITTED USES AND DISCLOSURES

• CEs are **permitted** to disclose PHI:
  – *Treatment, payment, or health care operations*;
  – *Public interest and benefit activities*;
  – *Incidental uses and disclosures*;
  – To the individual or personal representative (unless it’s a required access or accounting request);
  – Uses and disclosures with opportunity to agree or object; and
  – Limited data set for research, public health, or health care operations.

• *RFI requested feedback on whether treatment, payment and health care operations should be considered **required** disclosures instead of **permitted** disclosures*
PRIVACY RULE: TREATMENT, PAYMENT, AND HEALTH CARE OPERATIONS (TPO)

• **Treatment:** CE may use or disclose PHI for its own treatment activities, or of another health care provider.
  – *Example:* Consultations; patient referrals

• **Payment:** CE may use or disclose PHI for its own payment activities, or disclose PHI to another CE for payment activities of the entity that receives the information.
  – *Example:* Reimbursement of provider from health plan
• Health Care Operations:
  – *Examples:* Quality assessment and improvement activities; competency assurance activities; conducting or arranging for medical reviews, audits or legal services; certain insurance functions; business planning, development, management and administration; and certain fundraising activities.
    ▪ CE may use or disclose PHI for its own health care operations.
    ▪ CE may also disclose PHI for the health care operations of another CE involving quality, competency assurance activities, or fraud and abuse/compliance activities *IF* both CEs have or had a relationship with the individual and the PHI pertains to that relationship.
The HIPAA Privacy Rule permits uses and disclosure of PHI, without individual authorization, for the following 12 categories of public interest and benefit activities:

1. Required by law
2. Public health activities
3. Victims of abuse, neglect or domestic violence
4. Health oversight activities
5. Judicial and administrative proceedings
6. Law enforcement purposes
7. Decedents
8. Cadaveric organ, eye or tissue donation
9. Research
10. Serious threat to health or safety
11. Essential governmental functions
12. Workers’ compensation
PRIVACY RULE: INCIDENTAL USE AND DISCLOSURE

• Incidental use or disclosure is:
  – a secondary use or disclosure that cannot reasonably be prevented.
  – is limited in nature.
  – occurs as a by-product of an otherwise permitted use or disclosure.

• The CE must implement reasonable safeguards to limit unintended uses and disclosures and must implement the minimum necessary standard requirements.
PRIVACY RULE: INCIDENTAL USE AND DISCLOSURE (CONT.)

• The following are incidental uses and disclosures (assuming the CE otherwise complies with Privacy Rule) which are permitted:
  – an unauthorized person overhears a confidential communication between providers.
  – discussion of lab results with a patient or other provider in a joint treatment room.
  – oral coordination of services at a hospital nursing station.
  – utilizing sign-in sheets and calling out patient names in waiting room, so long as the information disclosed is appropriately limited.
PRIVACY RULE: INCIDENTAL USE AND DISCLOSURE (CONT.)

• The following uses and disclosures are **not** considered permissible as unintended/incidental:

  – an incidental use or disclosure that occurs as a result of a failure to apply reasonable safeguards or the minimum necessary standard
    ▪ for example, a hospital uses a waiting room sign-in sheet to ask a patient’s health history
  
  – erroneous uses or disclosures that result from mistake or neglect
    ▪ for example, posting a patient’s PHI erroneously on provider’s website
    ▪ for example, sending PHI to the wrong person by e-mail
PRIVACY RULE: MINIMUM NECESSARY REQUIREMENT

• A CE may only access or disclose the “minimum necessary” amount of protected health information.

• Where feasible, HITECH requires the health information used or disclosed to be limited to a “limited data set.”

• Where a limited data set does not contain enough information to conduct health-related business, HITECH allows broader uses and disclosures, but still the minimum necessary.

• Requirement does not apply (a) to patient treatment, (b) to disclosures to the patient; (c) to use or disclosure pursuant to a patient authorization, (d) disclosure to HHS for investigations, reviews and enforcement, (e) as required by law or (f) use or disclose to comply with other HIPAA rules.

• *RFI requested feedback on whether minimum necessary should continue to apply to care coordination and case management uses and disclosures
PRIVACY RULE: BUSINESS ASSOCIATES

• Recap of Definition:
  – An individual or entity that “creates, receives, maintains, or transmits PHI for a function or activity” on behalf of a CE or OHCA, but other than as a part of the workforce of the CE or OHCA.
    ▪ Example: Legal, actuarial, accounting, consulting, data aggregation, management, administrative, accrediting or financial services. Includes cloud service vendors, personal health record vendors or other vendors that provide data transmission services with respect to PHI on a regular basis.

• The term “business associate” includes subcontractors.
• Does not include persons with incidental access.
PRIVACY RULE: BUSINESS ASSOCIATE CONTRACTS

• CEs are required to enter into business associate agreements with BAs.
• Business associate agreements must impose specific obligations:
  – Only use and disclose PHI as permitted/required by agreement or as required by law (e.g., BA may use PHI internally for its proper management and administrative services or to carry out legal responsibilities). Cannot include use/disclosure that would violate HIPAA if done by CE.
  – Use appropriate safeguards to prevent use or disclosure of PHI.
  – Enter into a business associate agreement with subcontractors.
  – Report breaches.
PRIVACY RULE: BUSINESS ASSOCIATE CONTRACTS (CONT.)

- Mitigate breaches/improper uses and disclosures of PHI.
- Requirements re: access, amendment and accounting of PHI.
- Make books and records regarding HIPAA compliance available to Secretary of HHS.
- Certain obligations in the event of termination of agreement.
- Optional/Recommended if CE-friendly agreement: indemnification and insurance requirements.
PRIVACY RULE: PATIENT AUTHORIZATION

• Recap of General Rule: CE must obtain an individual’s written authorization to use or disclose PHI, unless it’s a use or disclosure required or permitted by the HIPAA Privacy Rule.
  – Psychotherapy Notes
  – Marketing: Any communication about a product or service that encourages recipients of the communication to purchase or use the product or service, unless an exception applies (e.g., face-to-face communication; gifts of nominal value; refill reminders; communication regarding alternative treatment for patient if the CE does not receive financial remuneration for making the communication)
  – Sale of PHI (unless the disclosure fits 1 of 8 exceptions)
PRIVACY RULE: PATIENT AUTHORIZATION (CONT.)

• Core Elements of Patient Written Authorization:
  – Description of PHI to be used or disclosed;
  – Who has the PHI;
  – Who will receive the PHI;
  – Purpose of the requested use or disclosure;
  – Statement informing patient of certain rights;
  – An expiration date or expiration event for the authorization;
  – The signature of the individual and date; and if the authorization is for marketing and the provider will receive remuneration from a third party, the authorization must disclose that there will be third party remuneration involved.
PRIVACY RULE: NOTICE OF PRIVACY PRACTICES

• Post Notice of Privacy Practices (NPP) prominently at premises and on websites
• Give copy to patient at first service delivery after compliance date
• Obtain patient’s Acknowledgement of Receipt of NPP
• Make copies available for patients to take
• Produce upon request
• Revise NPP for change in law, policies procedures, practice

• *RFI requested feedback on whether OCR should eliminate or modify the obligation for health care providers to obtain a written acknowledgement of receipt of the NPP
PRIVACY RULE: NOTICE OF PRIVACY PRACTICES (CONT.)

• Describe Patient Rights to:
  – Restrict
  – Access
  – Amend
  – Accounting
  – Alternative Communication Methods
  – Complain
### PRIVACY RULE: TIMETABLE FOR RESPONSES

<table>
<thead>
<tr>
<th>PATIENT RIGHT</th>
<th>TIMELY RESPONSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>30 days</td>
</tr>
<tr>
<td>Amend</td>
<td>60 days</td>
</tr>
<tr>
<td>Accounting</td>
<td>60 days</td>
</tr>
</tbody>
</table>

- *RFI requested feedback on whether the response time for access requests should be shortened*
ACCOUNTING OF DISCLOSURES

• Requires Covered Entities to track disclosures of PHI made in the past six years, EXCEPT for the following disclosures:
  – Disclosures for treatment, payment, health care operations
  – Disclosures to individuals
  – Incidental disclosures
  – Disclosures pursuant to an authorization
  – Disclosures through a facility directory or to individuals involved in an individual’s care
  – Disclosures for national security purposes
  – Disclosures to correctional institutions or law enforcement officials
  – Disclosures made as part of a limited data set
ACCOUNTING OF DISCLOSURES

- Under the HITECH Act (42 U.S.C. § 17935(c)), Secretary directed to allow individuals to obtain disclosures for treatment, payment and health care operations purposes made through an electronic health record for the previous 3 years.

- However, the HITECH Act qualified the directive with the following language:
  - “Such regulations shall only require such information to be collected through an electronic health record in a manner that takes into account the interests of the individuals in learning the circumstances under which their protected health information is being disclosed and takes into account the administrative burden of accounting for such disclosures.”

- OCR published proposed rule in 2011 that would have required Covered Entities to produce an “access report” detailing uses and disclosures of PHI through an electronic health record.

- According to OCR “commenters on the NPRM overwhelmingly opposed the proposed individual right to obtain an access report” and announced in the RFI its intention to withdraw the proposed rule without finalizing it.

- RFI asks for feedback on other ways to implement the HITECH Act’s directive on accounting of disclosures.
PRIVACY RULE: ADMINISTRATIVE REQUIREMENTS

- HIPAA privacy and security policies and procedures
- Designate a privacy officer
- Workforce training and management
- Mitigation
- Reasonable and appropriate administrative, technical and physical safeguards
- Complaint process
- Documentation and record retention
BREACH NOTIFICATION RULE
BREACH NOTIFICATION RULE: OVERVIEW

• Added under the HITECH Act

• The Breach Notification Rule requires CEs to notify every individual affected by a “Breach” of “Unsecured PHI” without unreasonable delay and in no case later than 60 days after “Discovery” of the Breach.

• BA must notify CE of a Breach without unreasonable delay and in no case later than 60 days after Discovery of the Breach.

• Rule contains content requirements for notice.
• In the event that the Breach involves PHI from 500 or more individuals from a state or other jurisdiction, the CE must also notify prominent media outlets in the jurisdiction.

• The CE must also concurrently notify the Secretary of HHS if the Breach involves 500 or more individuals or within 60 days of the end of the calendar year if Breach involves fewer than 500 individuals.
BREACH NOTIFICATION RULE: KEY DEFINITIONS

• “Unsecured PHI” means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary of HHS.

• “Breach” means the acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule that compromises the security or privacy of the PHI.

• There is a regulatory presumption that any acquisition, access, use or disclosure of PHI in violation of the Privacy Rule is a breach.
BREACH NOTIFICATION RULE: RISK ASSESSMENT

• Risk assessment to determine the probability that the privacy or security of the PHI has been compromised must be based on at least the following factors:
  – The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
  – The unauthorized person who used PHI or to whom the disclosure was made;
  – Whether the PHI was actually acquired or viewed; and
  – The extent to which the risk to the PHI has been mitigated.
Security Incident
Only EPHI
Includes *attempts* to disrupt information systems

Unauthorized Use or Disclosure
More inclusive than “Breach”
Does not take “probability of compromise” into account

Breach
Unauthorized uses and disclosures that compromise the security or privacy of PHI
ENFORCEMENT RULE
ENFORCEMENT RULE: OVERVIEW

• What triggers OCR enforcement?
  – Complaints
  – Breach Notification
  – Audits

• OCR enforcement may conclude in one of the following ways:
  – Finding of no violation
  – Technical assistance
  – Informal resolution – no civil monetary penalty
  – Settlement agreements – with monetary payments
  – Formal enforcement

• CEs and BAs must cooperate with OCR and permit access to facilities, books, records, accounts, or other sources of information.
  – Non-cooperation may lead to additional civil monetary penalties.
ENFORCEMENT RULE: PENALTIES FOR VIOLATIONS

• Penalty Tiers:
  – Unknowing ($100 per violation / $1.5M max)
  – Reasonable Cause ($1K per violation / $1.5M max)
  – Willful neglect ($10K per violation / $1.5M max)
  – Uncorrected willful neglect ($50K per violation/ $1.5M max)

• Potential criminal liability for individuals who knowingly obtain or disclose PHI in violation of the Privacy Rule

• Increased emphasis on enforcement and significant funding to support that activity
ENFORCEMENT RULE: $5.5M DATA BREACH SETTLEMENT

• In February 2017, OCR announced a $5.5M settlement
  – The settlement involved the operator of a hospital system
• OCR alleged that due to a lack of technical safeguards, the login credentials of a former employee of an affiliated physician’s office of the system had been used to impermissibly access ePHI maintained by the hospital system, potentially affecting 80,000 individuals. In particular, OCR alleged that the hospital system:
  – Lacked reasonable and appropriate access controls
  – Was not regularly reviewing its audit logs
CLOSING TIP: FEDERAL AND STATE PREEMPTION

• **General Rule:** State laws that are contrary to HIPAA are preempted, unless the state law:
  – Provides greater privacy protections of PHI.
  – Provides for reporting of disease, injury, child abuse, birth or death or for public health surveillance, investigation or intervention.
  – Requires certain health plan reporting, such as for management or financial audits.

• **Example (California):**
  – Written Authorizations
    - Cal. Civil Code § 56.11 requires written authorizations be no smaller than 14-point font.
  – Breach Reporting
    - Cal. Health & Safety Code § 1280.15 requires licensed clinics, health facilities, home health agencies or hospices to report unlawful or unauthorized access, use or disclosure of medical information within 15 days.
CLOSING TIP: FEDERAL AND STATE PREEMPTION (CONT.)

- **General Rule:** HIPAA does not pre-empt other applicable federal law. As a result, CEs and BAs may be subject to multiple federal enforcement regimes.
  - Examples:
    - 42 C.F.R. Part 2
    - 38 U.S.C. § 7332
    - Section 5 of the FTC Act
    - Fair Debt Collection Practices Act
QUESTIONS?

Scott A. Weinstein
Partner
sweinstein@mwe.com
(202) 756-8671
HIPAA Security Rule 101

Anne Kimbol, JD, LLM, CIPP/US, CHPC
Assistant General Counsel and Chief Privacy Officer, HITRUST

CONFIDENTIALITY COALITION
March 22, 2019 – Rayburn Office Building, Washington DC
INTRODUCTION TO SECURITY AND HIPAA
STATUTE LANGUAGE ON SECURITY
Importance of Security

• Even with the increased attention on privacy in 2018-19, security breaches continued to make headlines
• You cannot have an effective privacy program without good security
• Key security concepts –
  – Confidentiality,
  – Integrity,
  – Availability
Security Programs

- As we will discuss, HIPAA requires certain security measures be taken
- Additional measures may be appropriate as well depending on business type, size, and data collected
- Security must be a continuous process, with monitoring and updating as needed of policies and procedures
HIPAA Statute

• Requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards:
  – To ensure the integrity and confidentiality of the information;
  – To protect against reasonably anticipated threats or hazards to the security or integrity of the information, including unauthorized uses or disclosures of information; and
  – To ensure compliance with HIPAA security requirements
HIPAA Statute cont’d

Called for the Secretary of HHS to prepare rules addressing:
• Technical capabilities or record systems used to maintain health information;
• The costs of security measures;
• The need for training persons who have access to health information
• The value of audit trails in computerized record systems; and
• The needs and capabilities of small health care providers and rural health care providers
HIPAA SECURITY RULE
Background

- Found in 45 Code of Federal Regulations Part 160 and Subparts A and C of Part 164
- Officially the Security Standards for the Protection of Electronic Protected Health Information
- Rule was designed to protect health information while allowing new, useful technologies to be adopted and to recognize the different risks and resources available to covered entities
Scope

• Covers all electronic protected health information (ePHI); Privacy Rule includes all PHI - while written and oral PHI is not covered by the Security Rule, as I said before, you cannot have good privacy without security

• ePHI in motion and at rest

• All covered entities - HITECH Act lead to business associates having direct responsibility to comply with the Security Rule
Confidentiality, Integrity, and Availability in the Security Rule

- Confidentiality means ePHI is not available or disclosed to unauthorized persons
- Integrity means the ePHI is not altered or destroyed inappropriately
- Availability means that ePHI is accessible and usable on demand by authorized persons
Security Standards

• Flexible and scalable – Standards may be interpreted and implemented appropriately from the smallest provider to the largest plan

• Comprehensive - Cover all aspects of security-behavioral as well as technical – never underestimate the human factor

• Technology neutral - Can utilize future technology advances and new and innovative tools and systems

• Must cover administrative, physical, and technical concerns
Security Standards cont’d

- Entities must do a risk assessment to determine their own risks and the best mitigation measures; organizations are not given complete discretion, however, as they must have reasonable and appropriate measures in place.
- Organizations can determine their own technology choices to mitigate their risks.
- Key concept is “reasonable and appropriate”; consider:
  - Risk analysis and mitigation strategy
  - Current security controls in place
  - Costs of implementation – cost is not meant to free covered entities from their security responsibilities
Security Standards cont’d

• The Security Rule contains required specifications and addressable ones
• Addressable does not mean optional – must be reviewed to determine whether it is appropriate and reasonable for the entity and, if not, what else could be done to mitigate the risk
Risk Analysis and Risk Management

• A risk analysis is the foundation of any security program – until you know what your risks are, you cannot determine how best to mitigate them

• A risk analysis is an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity – entities have been found in violation of the Security Rule for not having a risk analysis at all or not having one that thoroughly covers all ePHI

• Risk management requires the implementation of security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the Security Rule

• Neither risk analysis nor risk management are ever really done – must be an ongoing process

• Toolkits have been released by the National Institute for Standards and Technology (NIST) and through a partnership between the Office of the National Coordinator for Health Information Technology (ONC) and the Office of Civil Rights (OCR)
Security Officer

“More than one individual may be given specific security responsibilities, especially within a large organization, but a single individual must be designated as having the overall final responsibility for the security of the entity’s electronic protected health information.” – generally known as the chief security officer
Administrative

• Security management (have a program)
• Personnel (properly trained personnel and an assigned security officer)
• Access management (only those who need access to ePHI get it; includes removing ex-employee user names and passwords)
• Workforce training (no specific timeline but many do annual; some state laws have timing requirements)
• Periodic assessment (check to make sure the program is properly implemented and provides the right protections)
Physical

- Access and control of facility (locks and badges)
- Workstation and device security (access to computers and other devices)
Technical

- Access control (make sure only people who are authorized to see ePHI can see it)
- Audit controls (see who is viewing what data)
- Integrity controls (keep ePHI from being deleted or changed inappropriately)
- Transmission security (safe while being transferred electronically)
How to Minimize Cyberthreats

- Comply with HIPAA Security Rule requirements
- Security controls in place
- Assess controls regularly
- Monitor threats
- Adjust controls accordingly
- Monitor internal system to ensure proper implementation of controls
BARRIERS AND ACTION IN DC AND BEYOND
Barriers and Potential Actions

• One of key barriers to strong security programs, particularly among small and rural covered entities and business associates, is resources.

• There has been discussion the last few years about creating safe harbors in the Stark Law and Antikickback Law to allow larger players to provide security tools to their smaller business partners.
Barriers and Potential Cont’d

• Another key barrier is the lack of qualified security workforce members. Encouraging the development of programs by universities and other educational institutions could help, along with possible student loan aid.

• Security is also often misunderstood. Encouraging the use of approved training programs and certification programs could help increase knowledge of the HIPAA Security requirements and industry best standards.
Current Legislative Action

• Senator Warner
  – Sent letters to healthcare associations and groups requesting information on improving cybersecurity in the healthcare sector
  – Responses are due today
• Discussion of security requirements as part of any federal privacy bill
• Numerous bills at the state level are pending in legislatures to address security
Questions?

Or email/call
anne.kimbol@hitrustalliance.net
469-269-1148
Visit www.HITRUSTAlliance.net for more information

To view our latest documents, visit the Content Spotlight